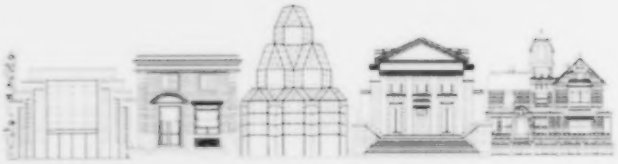
THE VIRTUAL DISPLAY CASE:

Making Museum Image Assets Safely Visible

3rd Edition

A report prepared for the



Canadian Heritage Information Network

by

Peter H. Roosen-Runge, Ph. D.,
York University

and

Anna P. Roosen-Runge,
Analecta Research & Resources,
February 2002

© Her Majesty the Queen in Right of Canada, 2003
Printed in Canada

National Library of Canada cataloguing in publication data

Roosen-Runge, Peter H.

The virtual display case : making museum image assests safely visible

3rd ed.
Issued also in French under title: La vitrine virtuelle.
Includes bibliographical references.
Issued also on the Internet.
ISBN 0-660-18790-6
Cat. no. Co61-17/2003E

1. Digital preservation.
2. Art objects – Conservation and restoration.
3. Cultural property, protection of.
4. Museum conservation methods.
I. Roosen-Runge, Anna P.
II. Canadian Heritage Information Network.
III. Title.
IV. Title : Making museum image assets safely visible.

AM145.R66 2003 069'.53 C2002-980064-1

Canadian Heritage Information Network (CHIN))
15, rue Eddy (15-4-A)
Gatineau (Québec) K1A 0M5

Tel. : (819) 994-1200
1 800 520-2446
Fax : (819) 994-9555
E-mail : service@chin.gc.ca
URL : www.chin.gc.ca

106-01417/

A Word from the Canadian Heritage Information Network (CHIN)

The Virtual Display Case, Third Edition, is an attempt to harness unique and emerging technologies, sometimes known in the market place as digital rights management solutions, that can be used to protect digital images in the on-line environment. It is by no means, an exhaustive overview. The first challenge faced by CHIN and the authors of this report is that it only addresses images as a form of intellectual property that can benefit from digital rights management solutions. Heritage institutions do not just work with digital images in the on-line environment. On-line exhibition production has increased to include audio and audio-visual files, 3D imaging and other new forms of media that are often more complex than a two dimensional image of an object in a collection. The second challenge faced by CHIN and the authors of this report is that by the time the report was ready for publication, the technologies may have evolved. Notwithstanding, we felt it necessary to at least publish a starting point for any museum professional embarking on digital rights management solutions in imaging on behalf of their institutions.

Opinion leaders working in the Internet environment have long debated whether this sort of technology is ultimately able to meet its objectives, particularly in the music industry. There is an adage in the industry that any technology that can be developed can also be hacked. And, as content developers in various commercial media grapple with the need to curtail on-line piracy, their appetite for new technologies to assist them in their fight against piracy increases. Technology developers try to meet the needs of the commercial market and hence much is said, reported, and published about their new products. But the emphasis is in producing the "next great thing" as opposed to embarking upon the systemic analysis and evaluation of the technology and the development of standards required to build long-term solutions. It is within this context that CHIN launches its Third Edition of *The Virtual Display Case* as a means of grounding the heritage community in order to provide some guidance on the very basic of all heritage digital content – the image.

Rina Elster Pantalony
Legal Counsel, CHIN

Table of Contents

8 **Preface to the Third Edition**

9 **Acknowledgements**

10 **1 Overview and Summary**

12 **2 The Context**

14 2.1 Museums On-line
15 2.2 Conservation Using Digital Images
16 2.3 Obligations and Hazards
17 2.4 Licensing as a Means of Education
21 2.5 Standardizing Licensing

22 **3 Digital Rights Management Systems**

22 3.1 Containers and Superdistribution
23 3.2 Rights Management Systems
24 3.2.1 ContentGuard
24 3.2.2 InterTrust
25 3.2.3 RightsMarket
26 3.2.4 OnDisC
27 3.3 Enforcing IP Rights Through Distribution Technology
27 3.3.1 Alchemedia and Vyoufirst

29 **4 Protection Technologies**

29 4.1 Varieties of Watermarking
30 4.1.1 Visible Watermarking
31 4.1.2 Invisible Watermarking
33 4.1.3 DCT-based Watermarking
33 4.1.4 Tracking the User
34 4.2 Encryption
35 4.2.1 Signatures for Authentication
36 4.2.2 Software vs. Hardware
36 4.2.3 Defeating Encryption at the Software Level
37 4.2.4 Interaction Between Compression and Encryption
38 4.3 Data Embedding Technologies
38 4.3.1 Cognicity
38 4.3.2 Digimarc
40 4.3.3 MediaSec
41 4.4 Secure Container Technologies
41 4.4.1 InterTrust's *DigiBoxes*
42 4.4.2 RightsMarket *RightsPublish*

44 **5 On the Horizon**

44 5.1 Rights Metadata and XML
46 5.2 JPEG2000
47 5.3 MPEG-4

49 **Sources**

56 **Vendors and Organizations**

Preface to the Third Edition

The rapid and continuous pace of technological innovation drastically reduces the useful life-span of almost any attempt to provide a summary or survey of technologies pertaining to digital images and their protection. It takes only a few months for bibliographic references to become obsolete, corporations providing products in the field to vanish or change their names, and new topics of significant interest to spring into view.

This edition represents a substantial revision of the previous version. We have eliminated references to issues and technologies that have been superceded or seem now to be of less importance, their place being taken by new developments in the information industry and in the management of digital rights.

The World Wide Web serves as an incredibly powerful tool to bring the reader directly into contact with current information on the whole range of technological and policy issues with which this report is concerned, so we have retained the practice of providing URLs as sources, wherever possible. But the same ready access and absence of rigid structure which makes the Web so valuable also gives Web-based information sources an ephemeral "here-today, gone-tomorrow" quality, which can be quite frustrating for the reader. We have attempted to verify that all the links currently listed are in fact valid, but that state of affairs will not last long. However, even if an individual link fails, the sites themselves may still have useful information, and with some judicious use of search engines, the reader may be able to find alternative and more current sources.

Acknowledgements

Grateful acknowledgement is made to Rina Elster Pantalony for her interest and assistance in preparing this monograph, and to Prof. Theodore Wilcox for his help with Section 5.2.

Trademark Notice

XrML, eXtensible Rights Markup Language and the XrML logo are trademarks of ContentGuard Holdings, Inc. Copyright © 2000 ContentGuard Holding, Inc. All rights reserved.

RightsXML™ is a trademark of TrustData Solutions Corp.

1 Overview and Summary

We present a study of the technological issues which arise from the possibilities of preserving and disseminating *digital images* of museum holdings, particularly the interplay between display and network technologies and intellectual property (IP) issues. The study is based on a review of the relevant literature, current commercial products, and on work on multimedia distribution and digital rights management by the OnDisC Alliance at Sheridan College, Oakville, Ontario.

As our title indicates, we are primarily concerned with the consequences of being able to distribute digital images, typically obtained from photographs through scanning or from a digital camera, over the Internet. But as Internet technology evolves, it becomes more and more practical to distribute much larger objects involving audio and video, and so we have expanded our scope to include some of the technological and IP issues that arise in connection with multimedia in general. In the past, the size and bandwidth requirements of multimedia restricted low-cost publication to CD-ROMs; today, we may safely assume that almost *all* distribution of multimedia to the general public takes place *via* the Internet.

While digital technologies create powerful new forms of preservation of text and images, and distribution of reproductions, they engender, at the same time, difficult problems involving intellectual property (IP) rights. There is a clash between the values of museums as cultural institutions and the marketplace, and this is paralleled by the clash between the altruistic values which caused the Internet to flower, and the desire to protect the economic rights legally inherent in created works.

It is becoming clear that amending and extending copyright legislation alone will not resolve such conflicts, if they can be resolved at all. In fact, in some ways, through the uncertainties of the law and the cost of testing it either as plaintiff or defendant, changes to copyright legislation have made matters more complex for both museums and copyright owners, as projects are abandoned or considered infeasible due to the complexities and costs of rights clearances. As a result, royalties and income to museums are foregone, and the level of educational and creative use of the works and objects in museum collections is diminished. Some of the difficulties can be alleviated by various forms of licensing to end-users, as is now routine in the software industry. However, the form of the licensing must be seen as appropriate and "friction-free" by the users, and licensors must pay some attention to educating end-users in the basic concepts of intellectual property.

Licensing, even if supported by registration, is viewed by some as providing too little protection for aesthetic goods that retain their value over a long period. Hence, the issue of protection of digital images has attracted considerable attention, and a number of technologies including watermarking, encryption, digital signatures, and fingerprinting have been developed and are being marketed. Recent developments, such as standardized forms of describing objects through metadata, the integration of encryption within new image compression formats, and the provision for persistent object identifiers stored within complex media presentations exemplify a trend in which the software used to create and transmit digital is increasingly required to take digital rights seriously, within the very structure of the media objects themselves.

In their current implementations, watermarks, signatures, and fingerprints have value primarily as deterrents to misuse and copyright infringement. Encryption can achieve high levels of security but even there the protection is never absolute and museums who implement such technologies must allow for the fact that there will be ongoing infringements, usually at low levels with little economic consequence. On balance, the best strategy in the short term may be to keep the burden of protection technologies as light as possible within the legal requirements, and secure protection against economic loss through simple user licensing agreements constructed and enforced on-line for specific works and for specific times.

In the long run, what will count for users is ease of access, variety, and comprehensiveness within a given domain. Since this is best achieved in a highly distributed, networked environment, in which there are no user-purchasable physical objects such as diskettes or CD-ROMS within which to fix the content—only licensable documents and performances—there arises an acute need for computer systems to manage effectively the digital rights. A software technology on which such systems can be constructed is under active development and deployment, in the form of *component software architectures*. Examples are the Microsoft Component Object Model (COM), "CORBA" (Object Management Group) and "JavaBeans" (Sun Microsystems). *Digital rights management systems* (DRMS) build *secure containers* of encrypted content out of the software components defined in these architectures, that contain within themselves the data and updating mechanisms used by the DRMS to enforce license terms, log usage, transmit royalty data to copyright collectives, and bill consumers. An example is the Microsoft Windows Media Rights Manager, [Microsoft, 2000] in which "COM objects are used to protect media files and issue licenses."

It appears that in the short term, container technology will be deployed most commonly in the context of electronic books and digital distribution of popular music, but we believe it has great importance for museums as it promises to solve the problem of re-distribution, by making the copying and retransmission of content, which today's protection technologies attempt to forbid, *no longer illicit but desirable* through the concept of "superdistribution". With superdistribution, a balance may be achieved between the cooperative/altruistic construction of aesthetic and educational content on the one hand, and the need to compensate creators on the other, allowing each museum's treasures to be put on display, even if only virtually, and to be viewed by a vastly increased audience.

2 The Context

Museums are entitled to feel that they are entering a "golden age"— over the last few decades, they became proficient in constructing exhibits and installations which combined photographs, text, film, video, and audio clips to instruct and entertain. And now, with fantastic rapidity, those very techniques find new, far more powerful expression in the digital domain, bringing the exhibit or installation to the desktops of individual "virtual visitors" at a school, or in a public library, or at home on the other side of the world.

At the same time, the assertion of property rights in the publication, exhibition or performance of created works, including all forms of imaging, becomes ever more vigorous and complex, creating an environment of uncertainty as to where and how museums can take advantage of the "golden" new possibilities. The gap between what is technically within reach and what is practical is clearly felt by museum professionals. A quote from a meeting of the Digital Image Access Project [1995] speaks to this frustration: "Of all the needs of the arts and humanities, the greatest is the need to get on-line access to images. We know there are billions of images and they are almost inaccessible. The technology to capture and display them is mostly here... .". But even if the funds were available to carry out the digitization and indexing, the issue of property rights clouds the vision of universal access to vast archives of images.

> "Few issues have hampered the creative development of interactive educational multimedia programs as [those associated with] intellectual property. Just the specter of an endless round of letters each asking for the permission to use a specific image, has kept many projects on the drawing board." [Trant, 1994]

Part of the pragmatic resolution to the frustration created by the technology will come from the technology itself. The museum's traditional display cases protected the museum's holdings from damage and theft, while allowing visitors to see as much as possible of the contents. As museums increasingly avail themselves of digital technologies to create image archives and multimedia presentations, they will be able to exploit new forms of "display cases", primarily in the form of computer software which make their contents as visible as possible over easily accessible networks, while protecting the images and presentations from unauthorized copying and publication.

Fortunately, tools and techniques in this area are developing rapidly to meet the needs of commercial interests in expanding markets for all forms of digital media, particularly through the delivery of new media over networks, and some of these approaches will have relevance to the protection of on-line museum materials. This confirms a trend, noted by Gurrian [1995], which finds museums aligned with other entities in new classifications which include not just the traditional libraries, archives and schools, but also "technologically-based storehouses", e. g., image databanks.

Current nation-wide initiatives encourage the initiation and continuation of digitization projects, which in turn stimulate the development of digital depositories. As these digital depositories grow larger, the content becomes much more useful and provides a greater incentive for participants to

contribute multimedia material such as audio and images which were previously unavailable to the general public. A Canadian example is provided by the BELLE project to create and populate a searchable database of multimedia content for use by post-secondary educational institutions for distance learning. Project participants are universities and colleges located across Canada, connected by a multimedia server infrastructure concentrating on the speed and quality of delivery. The project offers users access over a broadband delivery system to high-resolution video and 3-dimensional image files that currently cannot be viewed using conventional networks due to their unwieldy large bandwidth size. By focussing on accessibility, searchability, flexible usage, and stable network resources, the BELLE project will help stimulate the development of accessible Canadian museum community Internet-based education and outreach programs.

Another example is the European Commission's Info2000 projects, which aim to stimulate the development and use of multimedia content. A specific instance is the European Visual Archive (EVA) project [van Horik, 2001] which has developed a detailed and systematic approach to increasing access to historical photographic collections through documentation and digitization. In this effort, commercial exploitation is not a main concern—the goal has been to create a system with a "low participation threshold" enabling European image collections "to get in contact with a huge potential of image consumers".

Museums will need to adapt to the easily accessible presence on the Internet of commercial providers of image content seeking to sell reasonable high-quality images not only to commercial artists, and publishers, but also to schools, and eventually individuals. Storm [1995] has urged libraries and archives "to step back and . . . analyze how they will, and are being, affected by the advent of commercial networked information services".

An interesting example of such a service is the Corbis Corporation [Lieber, 1995], which, supported by the wealth of Bill Gates, aggressively seeks to acquire "electronic" rights, often exclusive rights, to the digital imaging of the holdings of art museums and image archives such as the photographs of Ansel Adams. With its purchase of the entire Bettmann Archive in 1995 and the 1999 purchase of the Sygma news photography agency, Corbis now holds the rights to over 65 million images, including 2.1 million in digital form [Reuters, 1999]. As M. Hallacy has commented, "Gates has effectively acquired the rights to the photographic record of history. . . These rights include the ability of our culture to reproduce ourselves." Corbis holds rights to the digital archives of many large museums including the Hermitage in St. Petersburg, the National Gallery in London, the Seattle Museum of Art, the National Gallery of Art and the Corcoran Gallery both located in Washington, D.C. [Hallacy, 2000]. Other Corbis ventures include Corbis Sharpshooters, specializing in photographs of people, lifestyles and nature, and Corbis Saba, which represents editorial and portrait photographers. In January, 2002, Corbis acquired moving image company Sekani (www.corbis.com).

By comparison, the Art Museum Image Consortium (AMICO) digital collection provides about 65,000 art images to its members who participate in a cooperative digitization, licensing and distribution agreement. The Virtual Museum of Canada makes about 200,000 images from the collections of its museum members freely available to the general public. Membership agreements outline roles and responsibilities for this collaborative undertaking.

2.1 Museums On-line

Museums of all sizes are creating websites in rapidly increasing numbers, with great enthusiasm. For a small museum such as the Berea College Museum, the motive is clear: audience and students. As Chris Miller reported on MUSEUM-L (9-Apr-1996):

> "on-line exhibition is a viable way to expand your audience into new sectors. We are a small college museum, focused on Appalachian history and culture, and located in a rural community. Almost every visitor who visits 'Gallery V (for virtual),' our on-line gallery, would not have come to the museum in person. Almost 25% of our on-line visitors are international. There are people in Ecuador who are interested in Appalachian Culture who cannot come to our museum. For them, any encounter with the stuff is better than no encounter at all."

For the larger museums, there may be more question as to the value of virtual galleries compared with the value of "seeing the real thing", but they too appear on-line in ever increasing numbers. "The WWW [World-Wide Web] offers a relatively cost-effective means for the [Canadian] Museum [of Civilization] to disseminate its information resources to a wide range of audiences; . . . use is spreading into the school system, thanks to projects such as Schoolnet." [Alsford, 1994]

The National Palace Museum in Taiwan has created a website offering virtual tours to highlight their collection and exhibits. Based on a clickable floorplan, the viewer is taken to rooms or areas in which they can 'walk' around in 360 degrees, using the QuickTime plug-in of their web browser. You can even get 'out of' the taxi cab in which you virtually arrived! A virtual 'painting' of the Palace itself is accompanied by a detailed description of the painting, the present condition and an explanation of its context comparable to the content of an audio guide for an actual exhibit.

A telling indicator of the importance of the museum community on the Internet and the Web is the decision of the Internet Corporation for Assigned Names and Numbers (ICANN) to include in the top-level Internet domains the new domain *.museum*.

There is currently an interest in funding programs for creation of online cultural material. The proposed Culture Online initiative of the Department for Culture, Media and Sport in the UK, would aim to "use digital technologies to widen access to the resources of the arts and cultural sector...." (www.cultureonline.gov.uk)

In Canada, the *Virtual Museum of Canada* features a branded collection of high-quality content and features developed by museums and their partners. The *Virtual Museum of Canada* is an initiative of the Canadian Cultural Online funding program, created to "develop the capacity of Canada's cultural industries, institutions, creators and communities to produce and make available on the Internet the digital cultural content that will help promote Canada's rich culture, history, arts and heritage and encourage shared values amongst Canadians" (http://www.pch.gc.ca/ccop-pcce/main_e.cfm). The Virtual Museum of Canada site averaged over 200,000 visits per month in its first 10 months of existence. One of the principals of the VMC is that intellectual property rights must be respected, and partners must ensure that they have or clear the rights to all information elements included in on-line presentations.

The Canadian Heritage Information Network (CHIN) offers a digitization course to museums considering a digitization project, entitled 'Capture Your Collection'. Working towards creating a more savvy museum community, the 9-part course contains a section entitled 'Legal Issues' focussing on the legal implications of undertaking an institutional digitization project and the need for security concerning the display and use of digitized material. [CHIN, 2000]

Increasingly ambitious projects to create on-line image libraries have appeared in the areas of science, art and history. The Van Eyck project describes its mission in these terms:

> "The vision that inspires the VAN EYCK Project is a world wide network of Art History Library Photo Archives which together would provide an unparalleled resource base for research and study. Such a network would reach a critical mass with the co-operation of as few as ten of the leading Art History Photo Libraries in the world. This would be facilitated by the existence of a relatively small number of leading centres such as the Courtauld Institute's Witt Library, the RKD and the Marburger Index with holding of images, associated scholarly material and practical information on millions of works of art. . . . " [Van Eyck Project, n. d.]

The goal of digital libraries with millions of images accessible to the Internet is not a distant one; the Library of Congress's "American Memory" project contains (at this writing) five million digitized images.

We draw two conclusions from such developments:

- Museums and archives will increasingly be expected by the public to appear on-line, and with more and more content. Museums which merely advertise exhibitions or promote their holdings without revealing any will not attract repeat visitors. Archives will be expected to maintain their content in a form so that users over the network can find it with appropriate tools such as Web search engines (at present the most powerful, if rather blunt-edged, retrieval tools available), and view, print, listen to or otherwise use that content.

- But this on-line distribution of content increases the responsibility of digital archives to manage intellectual property rights by facilitating transactions between rights-holders and users, and by taking every reasonable precaution to prevent unauthorized use of the distributed material.

2.2 Conservation Using Digital Images

The development of digital imaging at higher and higher resolution, and the ability to use technologies such as Photo CD [Smith, 1994] to store the resulting images reasonably permanently on CD or DVD-ROMs, produced cheaply within the museum or archive itself, provides a powerful impetus for creating digital archives of text, manuscripts, maps, etc., and has removed some of the earlier objections to digitization [Weber, 1993].

As more and more materials are preserved through such tools, care will have to be taken to stay within the restrictions of copyright.

The 1998 amendments to Canadian copyright law specify in what circumstances images may be copied (increasingly into a digital form) for preservation:

- if the original is rare or unpublished and requires conservation,
- to allow on-site consultation if the original cannot be used because of its condition or because of the atmospheric conditions in which it must be housed,
- if the original is in an obsolete format or if the technology required to use the original is obsolete,
- or if necessary for restoration [Harris, 2000].

2.3 Obligations and Hazards

Broadly speaking, a museum or archive is obliged:

- to protect the commercial value of images for which the museum holds the copyright.

Traditionally, this was done through the threat of legal action against infringers, but it is becoming increasingly obvious that in a digital, networked environment, in which most of the potential infringers are end-users—"visitors" to the museum—reliance on legal sanctions alone will be counter-productive.

- to ensure that the museum meets its legal obligations to copyright owners for images which it owns or licenses, but for which it does not hold the copyright.

The hazards of copyright and ownership are real: a posting to MUSEUM-L [Keshet, 1996] described a lawsuit involving a colour transparency of a single work in a collection of art works owned by a museum, the copyright for which (unknown to the museum) the artist, now dead, had assigned to a third party over 60 years ago, making the museum's photographing the work an infringement, and its licensing of the transparency to a publisher doubly so. Unfortunately, the question of who, if anyone, has a valid claim to the copyrights associated with a work may have no definitive answer in advance of judicial determination; as an example, the European Visual Archive report on copyright issues [EVA, 1999] lists no less than five differing expert opinions on when photographs are covered by United Kingdom copyright and by whom.

- to ensure the integrity and authenticity of reproductions made available to the public either by the museum or "third parties".

The problem here is especially acute because of the ease with which any form of digital information can be copied, manipulated, and redistributed. Inexpensive but powerful desktop software makes it possible that almost anyone with limited knowledge can duplicate, manipulate and print images, thus making copyright infringements easy to carry out, and extremely difficult to police. Additionally, the nature of publishing nowadays requires images in a digital form, so that, for example, if photo agencies supply only transparencies, it is almost certain that the clients will themselves digitize the images for ease of use in their publication software. Kodak itself, in advertising its Photo-CD image storage technology, has promoted its value in terms of the ease of image manipulation:

> "With applications such as Adobe Photoshop you can change [the Photo-CD] images in virtually any way to fit your particular need. Restoring old photographs, placing people in pictures, or removing unwanted items are just the beginning of what you can do."

Museums which display selections from their holdings on a website have often relied on the use of *thumbnails*—reproductions so reduced in size and quality that there is no value in copying them—as a way of avoiding the problems of easy copying and redistribution. This also had advantages in the context in which disk space was expensive and the downloading of an image file to a user's browser was likely to be quite slow. But the continued technological improvements in scanning, storage and delivery make it now practical to offer users a much higher quality of visual experience, thereby raising user expectations. For example, the State Hermitage Museum, St. Petersburg, Russia, has used the IBM Digital Library system to create a gallery of digitized images entirely accessible to the user at high resolution through a browser:

> "The Hermitage's decision to make its whole online collection available at high resolution – instead of providing just a few high resolution images as most museums do – makes sense to Fred Mintzer, who leads the [IBM] group. 'At first glance, that kind of image quality might seem higher than necessary,' he says, 'but it must be provided in order for the Website visitor to begin experiencing the beauty of the art.'" [Stewart, 1999]

It is also significant that in this case the gallery viewer views the digitized objects without downloading any special software that could enforce a licensing agreement with the museum.

It is not clear under what rights and permissions the Hermitage Museum is able to make its images available in this way, but in the Canadian context, an important issue would be the exhibition rights given to creators by the amended Copyright Act (RSC 1985, c.C-42, as amended) of 1988 [Rottenberg, 1997]. It is likely that almost any way of making a digital image of a work created after 1988 available for viewing over a publicly accessible network counts as an "exhibition" and requires permission of the copyright holder.

Greg Spurgeon of the National Gallery of Canada has commented that the exhibition right

> "has brought the will of most galleries to support the moral and economic rights of creators into conflict with their own ability to promote and exhibit contemporary art in the face of these new financial and administrative obligations. Some have set up the necessary mechanisms to negotiate and pay the exhibition fees (though this is an ever-increasing administrative burden at a time of wide-spread down-sizing in museums); and some continue to investigate means of licensing exhibition and other rights in a manner that respects the rights of the creator/copyright holder without imposing on the museum a burden which would inhibit its ability to carry out its mandated programmes." (MUSEUM-L, 11 Apr 1996.)

2.4 Licensing as a Means of Education

People often assume an implied right to copy, print and further distribute any material found on the Internet. The assumption that it is all right to copy is often justified by appealing to the fact that many of the tools we use for e-mail, or to access newsgroups, or to ftp a document from an archive, as well as much of the content itself, has been constructed by altruistic labour. It is not uncommon to see new material posted to the Net or an FTP archive with the comment that it is made available in the tradition of "giving something back to the Net".

In this spirit, the US-based Internet Moving Images Archive, a non-profit initiative which contains digitized material relevant to 20th Century American social history, posts its video catalog of over 1000 titles in downloadable files on its website. These files are available for free and without any restriction "other than that the films cannot be resold or licensed by anyone in their entirety or as stock footage." [Internet Archive, 2001].

Despite the commercialization of the Internet, public domain resources still exist. Some US institutions—notably, NASA—make large collections of scientific and historical images available without restriction. An example is the Dryden Research Aircraft Photo Archive, containing digitized photos of research aircraft images dating from the 1940s to the present, for which, *explicitly*, no copyright protection is asserted. In the case of the Library of Congress "American Memory" collection, the Library provides information about copyright owners and other restrictions but leaves to the user the determination of what uses of the images are appropriate.

In the world of software publishing, we have become used to the phenomenon that customers and publishers are obliged to enter into contracts. As Strong [1994] observes:

> "This has never been the case before. The typical transaction between a publisher and a customer occurred in a bookstore where the customer plunked down money and walked out with the product. As the publisher/customer relationship becomes closer, it will either become more hostile or it will become more interactive and more mutually educational."

Howard Knopf, a leading Canadian copyright lawyer, [Norman, 1995], has warned of a backlash if fair use or fair dealing is eliminated or substantially restricted. "The laws must persuade and not threaten. . . Too much copyright protection could well stop the information highway dead in its tracks". The issue has become particularly contentious in the area of digital distribution of popular music, under the industry-designed provisions of the US Digital Millennium Act. A specific criticism has been that

> "content owners and digital rights management companies are discouraging the growth of digital music by taking liberties with their control of copyrights" [King, 2001],

with critics, such as Princeton professor Edward Felton, arguing that rather than focussing on creating convenient ways for consumers to pay for content and developing piracy tracking applications, the major content companies have been pushing to gain "unprecedented control over copyright" itself to block user rights previously available.

On the positive side, image distributors now increasingly make available links to on-line information about copyrights and copyright legislation, for those users who desire further details; much more can be done along these lines using the powerful interactivity of Web servers and browsers. In this way, providers can explain and educate users as to the nature and purpose of copyright.

As an example, the Bridgeman Art Library, a large commercial digital image distributor from the UK, places the copyright information regarding use of its images prominently on the main navigation bar for the entire website. The link takes the user directly to a list of recent articles about copyright and images on the Web and then to a page from which the user can select the intended use of the images: academic or personal interest, or editorial or commercial. When the user selects the type of use, a detailed explanation of the user's responsibilities is shown [Bridgeman, 1999].

The Art Museum Image Consortium (AMICO) Library at the University of Alberta uses the same webpage with which users gain access to the database to explain its conditions of use:

> "access to and use of the AMICO library is exclusively for education, research and scholarship. ...The AMICO library may be used for (1) classroom instruction and related activities, (2) student assignments, (3) public display...in a university museum, gallery or similar facility..., (4) public display...as part of a professional presentation...,(5) use in a student or faculty portfolio..., and (6) use in a dissertation..." [University of Alberta, n. d].

It is significant that positive conditions matching the needs of the intended users are explicitly presented, along with restrictions of which the users should be aware.

As part of the SchoolNet Digital Collections, the Parks Canada website includes an image gallery for students. The image use information is presented in plain language aimed at a child user. A link from the main webpage explains how students may use the images:

> "The images you will find here come from a vast collection of images owned by Parks Canada. You can download, save and print any of these images for use in your school projects or just because you like them! "

The explanation also includes a section regarding the definition of copyright as it is applied to the gallery images:

> "What does © Parks Canada mean? That simply means that Parks Canada owns each of the images included in 'Images of Parks Canada.' You are free to download, save and print any of these images for your school work." [Parks Canada, n. d.]

The Copyright statement on the *Virtual Museum of Canada* site outlines accepted uses of the material on the site:

> Copyright
> Unless otherwise noted, all materials that are part of this Web site, including images, illustrations, designs, icons, photographs, video clips, and written and other materials are copyrights, trademarks, trade dress and/or other intellectual properties owned, controlled or licensed by Canadian Heritage Information Network (CHIN) or its member museums.
> We invite you to use the material on this Web site for educational and personal purposes. Copyright and other propriety notices should be kept intact with the material.
> Express permission from CHIN or other indicated copyright owners is required if you wish to modify, copy, reproduce, republish, post, transmit or distribute the material in any way for any other purposes, especially commercial.

For digital material, the terms of a license granting access to the material are often more significant in controlling usage than the provisions of copyright legislation. In the academic communities, the issue of licensing as a method of granting protected and restricted access to archival material has become quite controversial, as it is seen as undermining the traditional 'fair use' rights of access (in U. S. copyright law) and copying for scholarly purposes. This is not the case in user-oriented licenses such as AMICO licenses which explicitly state that they do not limit 'fair use' and permit uses that go beyond it [AMICO FAQ, n. d.]. But in general, "licensing trumps fair use" [Snow, 1997], as has become very evident as a result of the controversial provisions of the U. S. Digital Millennium Copyright Act which came into effect in October, 2000:

> "criminalizing the act of circumvention of a technological protection system put in place by a copyright holder — even if one has a fair use right to access that information. . . Consequently, the [American] public will have fewer rights in the digital realm than it enjoyed in traditional space to use and access information." [Gross, 2000]

The concern that this has raised on the part of libraries and educational institutions generally, is shown by the American Library Association's comment that

> "Over the long term, these technological 'locks' could have an enormous impact on the ability of libraries to provide access, lend, and archive materials, as well as the ability of library users to make full use of resources." [ALA, 2001]

On the other hand, it is possible that museums will be unable to assert copyright over digital images of art works in the public domain precisely because such images literally reproduce objects and thus do not contain an ingredient of originality required to create a work which can be protected by copyright! This is the finding in a case decided in 1999 against the Bridgeman Art Library in the US (but under British copyright law) and in favour of Corel Corporation over a CD-ROM containing digital reproductions of well-known paintings by European masters which included 120 works of art which Bridgeman claimed to have the sole authorization to control. The museum implications of this decision are described by American Association of Museums Government Affairs Counsel, Barry G. Szczesny:

> "Bridgeman raises concerns for proposed enterprises such as Museum Digital Library Collection (MDLC) and the Art Museum Image Consortium (AMICO). . . [A] legal memorandum on this issue to see what options are out there for legally protecting digital images of public domain works in a post-Bridgeman world recommends a combination of:
>
> 1. introducing creative variations into the digitization process to increase the chances of the digital copies qualifying for copyright protection (but this would defeat the purpose of provided a true reproduction);
> 2. assembling digitized images in a collection may provide copyright protection to the collection as a whole, just as would providing value-added text and documentation, but will not protect the underlying works if they are not independently protected;
> 3. seeking to impose contractual restrictions upon subsequent use of the digital copies through licensing (but note a contract will not bind a third-party user who obtains the digital image); and
> 4. exploring the possibility of placing technological restrictions on copying. This is the most practical measure.
>
> What may be most important for museums is to do a better job of educating the public about the rights and reproductions enterprise. " [Szczesny, 1999]

The Bridgeman decision may also have implications for the way in which universities license digital image collections. A license restricting access to a specific network, as illustrated in this notice from the University of Indiana's Dido Image Bank:

> You don't have access
>
> For copyright reasons, images in the Dido image bank can't be accessed from outside the Indiana University Bloomington network.

would still have effect, but if an instructor at the University were to make copies of a set of images from the Dido database and make them available to her students, it appears that this might not be a copyright infringement (see point 3 above.)

It remains to be seen how these issues play out in Canadian jurisprudence or its future amendments to Canadian copyright legislation, which are already needed to extend its current limited treatment of "reprographic reproduction" (i. e., digitally scanned as in a photocopier, but only on to paper, as opposed to a computer file) to cover works stored and copied in digital form.

2.5 Standardizing Licensing

A significant step forward in creating forms of licensing that enable museums to more effectively fulfill their mandate for dissemination, while protecting intellectual property, is achieved through a consensus about practical "accepted practices", through the development of standard license agreements [CHIN, 1997]. The AMICO project of the Association of Art Museum Directors has made a significant contribution to this effort by establishing a detailed framework of rights, permissions and usage restrictions for digitized images. [AMICO, 1998] As many of the "customers" for broad access to museum content in digital form are educational institutions, it seems likely that museums will feel the impact of the trend on the part of those institutions to form consortia which can, through larger scale licensing, achieve more favorable terms with respect to usage and cost then could be achieved by individual sites. A prime Canadian example, the Canadian National Site Licensing Project (CNSLP) [Schofield, 2000], focusses on licensing full-text electronic journals and research databases, primarily in science/technology/medical disciplines, but the lessons learned may, at least to some extent, be ultimately be applied by universities and colleges to negotiating site licenses with museums and museum collectives in Canada.

The attitude towards licensing vs. sale is clearly evolving. The Digitization Project at the Canadian Museum of Civilization which began in 1993 had as its initial intention to sell the digitized images, but the experience of the Museum suggests that licensing may be a better use of the resource. From a databank of over 300,000 digital images

> [...] less than 1,000 of them have been sold as originally intended, although more have been licensed for use. [Tomlin, 2000]

The development of standard license agreements will, in itself, not be sufficient to make the exhibition and distribution of digital images generally practical. Museums will require, in addition, management systems and associated databases, recording on a continuing basis the hundreds and thousands of license agreements to be executed in the future regarding images of copyrighted works. Such computer systems are known as *rights management systems*; they constitute our focus in the next section.

3 Digital Rights Management Systems

A number of emerging technologies may be able to mitigate the need for self-defeating and alienating legalisms. The overall framework is provided by *digital rights management systems* (DRMS), understood as networked, remotely accessible databases which combine data on users, content originators, licenses and usage, to restrict and enable user access to information delivered over a computer network. Such systems can greatly reduce transaction and licensing costs, making it much easier to charge and collect reasonable fees for content of commercial value, while enabling providers to allow other content to be accessed at nominal or no cost. This should allow museums (as well as other providers of educational multimedia content) to more easily obtain presentation or exhibition rights for images and other media. [Hoffert, 1996]

The beginnings of rights management systems at educational institutions, applicable to a museum context, are found in currently available *license-servers*: system software which keeps track of how many copies of licensed software are currently being executed in a lab or on a local-area network. Such systems are inadequate to handle the complex licensing and reporting requirements needed to handle online distribution from multiple publishers with a variety of usage conditions. For this reason, DRMS software has become a complex, multifaceted product, as illustrated by the examples later in this section, and so is likely to be installed and maintained centrally at an institutional level, rather than at the level of a lab or department.

3.1 Containers and Superdistribution

Rights management systems must convince owners that their property is secure and will not be re-distributed. Until recently, there has been no practical way to achieve this; as Harland Cleveland [1985] observed, information, if valuable, is inherently leaky because the cost of leaking (copying) is tending to 0. But this is no longer true if content is encapsulated in an unbreakable (i. e., encrypted) software "container" which permits itself to be copied for free but requires some transaction such authorization, registration, agreement to pay, etc. before its contents can be accessed.

Such containers enable a process known as *superdistribution* [Cox, B. 1996], in which content can be freely copied and re-distributed without causing economic harm to the copyright holders. In fact, the copying provides an economic *benefit* to them since it makes it possible for more users to acquire the container, comply with the license requirements, including payment, in order to get permission to access the container. (Ironically, superdistribution licenses will need to *exempt* users from copyright infringement when they copy the containers for re-distribution.)

A museum, for example, may in the future, construct an exhibit from many interactive sub-components, including, for example, licensed images of other museums' objects as well as those it owns itself, copyrighted text, sound clips whose performance rights belong to their composer, etc. All of these components would be obtained by the museum (probably over the Internet), as encrypted containers. The museum would then use appropriate software tools to combine its materials (also 'containerized') into a single presentation or interactive application, which it freely distributes to consumers ("virtual visitors") over the Internet for a specific period of time. It is thus distributing its own material and re-distributing the material of others at very little cost to itself.

Users of the museum's product will interact over the Internet with a rights management or intellectual-property management system which will handle the licensing, payment, etc. not only for the outer container constructed by the museum, but for all the sub-containers which were obtained from other sources. These sources thus may obtain royalties without any direct involvement on the part of the museum in the transfer of rights, permissions, or funds.

3.2 Rights Management Systems

To illustrate what content providers, such as museums, can expect from rights management systems, we consider briefly the general features which are found in any large-scale system suitable for distributing images or, more generally, multimedia, and then look at several specific systems which are currently available or are under development:

- ContentGuard
- InterTrust Virtual Distribution Environment
- RightsMarket
- OnDisC

General Features

- *Access Control*: a registry of user credentials and profiles to perform "access permissions evaluation" which determine user rights to access information sources.

- *Authentication:* to validate the user's identity. Authentication in most Internet-based transactions today occurs through the use of a user ID/password assigned to a user as part of a registration process. But authentication for electronic commerce will increasingly use unforgeable digital IDs, or certificates, which validate that you are who you represent yourself to be, as well as your affiliations.

Authentication also applies to the information provider's document server (e. g. a museum's Web server) which is intended to communicate with the rights management system, to avoid the problem of "spoofing" in which a computer ('host') attached to the Internet has been programmed to identify itself as another host.

- *Browsers*: All transactions are transmitted over the Internet using the now-standard Hypertext Transfer Protocol (*http*) protocol [Berners-Lee, 1994]. Secure transactions between the browser and the servers use security features based on encryption, built into the browsers, such as Netscape Navigator/Communicator which supports the Secure Sockets Layer (SSL) protocol.

The capabilities of a user's browser can be extended through the use of "plug-ins"—small pieces of software downloaded over the Internet to the user's computer. A plug-in for a rights management system can be used to handle the " buy" transaction by a consumer, and extract the decrypted document from an encrypted "container", to make it available to the browser. (Encryption and container technology are discussed in more detail in Section 4).

- *Custom applications*: A vendor or distributor of protected content may wish to provide the user with a special interface to replace the browser. To avoid dependencies on the user's hardware and operating system, such applications can be coded, using the widely-available Java language, in the form of *applets*, which are automatically downloaded over the Internet when needed, and then disappear from the user's machine after use. An important feature of applets is the ability to control what operations the user is allowed to perform on the protected content, such as printing and saving, based on the user's license or permissions.

- *Clearing Center*: A large-scale rights management system requires a clearing center to provide accounting records of use, payments, licenses granted, and the registry of new content.

- *Identification:* For multimedia content, identification of the source (creator or publisher) embedded in the content in the form of visible or invisible watermarks is increasingly seen as an important form of protection. (See Section 4.1) Distribution information which records receiver identification can also be hidden in the copy of a document transmitted to a user to deter further unlicensed re-distribution.

3.2.1 ContentGuard

ContentGuard™ provides an example of the type of commercial digital resource management products available to organizations that wish to maintain highly detailed control of the usage of their content. The owner of the content, the institution, sets up the rights policy on the digitized information to cover use of the content in the widest sense. Using metadata expressed in a proposed specification language, XrML™ (see section 5.1), to enable "rights labelling", the content owner can specify what rights the user has to the content and the conditions under which those rights are allowed. The rights label contains all of the conditions of content use, such as the fees to access the content and the time span of use. It also contains summary information concerning the content and is used to create the license issued to the content user. The content owner has total and customized control over the user's ability to print, view, save, alter, copy, or rebroadcast the content.

This approach to wide-reaching content management implements a form of superdistribution, in that, when content containing a rights label is emailed or otherwise distributed from a licensed user to a non-licensed user, access to the content is refused. The non-licensed user then is directed to the content provider's website to obtain legitimate access. Contentguard calls this process "persistently enforced rights".

ContentGuard currently protects text media (files such as HTML, XML, Quark, PDF, Word and Excel) and is developing products to similarly protect audio and video.

3.2.2 InterTrust

InterTrust Technologies has patented a number of inventions pertaining to information metering, distributed data security, superdistribution, and digital rights protection, which provide the basis for

what it calls "the InterTrust Virtual Distribution Environment™ technology to support unmet, critical needs of electronic commerce". Rather than offering a product or system, InterTrust licenses a set of tools for developers of rights management applications.
InterTrust uses container technology to provide secure content containers for distributing information, so that the information can only be used in conformity with rules and controls, specifying what types of content usage are permitted, as well as the consequences of usage. But the InterTrust architecture does not rely on central servers to distribute content. Instead, independent decoupled InterTrust-enabled systems exchange rights, licenses, keys, etc., as well as content, using secure software containers called DigiBoxes™. (See Section 4.4.1.)

The InterTrust technology works by integrating its procedures directly into the operating system of a computer or applications or by extending the system, to create a protected operating environment: an "InterTrust Commerce Node". It is likely that, in the near future, this will not be necessary, as operating systems begin to directly support the rapidly evolving concept of *component software*—software objects constructed from small, reusable building blocks which can independently access applications and operating system resources.

Components are a natural form for software containers, and as the InterTrust technology demonstrates, secure information containers are likely to be a key enabling technology for superdistribution.

3.2.3 RightsMarket

A Canadian entry into the rights management marketplace is the *RightsMarket* system (discussed in more detail in Section 4.4.2). This system creates a number of databases to support rights management, specifically:

- contracts between consumers and publishers or distributors running the RightsMarket software,
- billing information (which can be maintained on the customer's computer as well as at the distributor), and
- artifacts (digital objects) available for distribution and requires a Windows application to be installed on the user's machine.

Artifacts can be distributed in a variety of ways, through the Internet using a conventional browser, or on a physical medium such as CD-ROM. Artifacts are processed through a RightsMarket "wrapper factory" which encapsulates the product, requiring the user to have a "trusted viewer" in order to open and use the contents. As with ContentGuard, the RightsMarket technology enables protected superdistribution.

In its current implementation, the protected content must be served from a server maintained by RightsMarket. RightsMarket also controls the database of users and usage, which it uses to authenticate licensed users, and from which it generates accounting reports for content providers.

3.2.4 OnDisC

OnDisC Research Group, an alliance of digital content owners and post-secondary institutions, is developing tools to manage the distribution of multimedia digital content for educational purposes. The project prototype consists of online "coursekits" of digital material for distribution to students. This project, based at Sheridan College, Oakville, Ontario, will be initially tested in Ontario educational institutions and then extended nationally, using the CANARIE high-speed education/ research network.

The objectives of the OnDisC project are to demonstrate the construction of a "union catalogue" for digital content from a variety of providers for distribution to instructors and students at variety of post-secondary institutions, integrated with the management of the associated digital rights, including usage tracking.

In the OnDisC system, instructors create "coursekits" by selecting digital content from the catalogue available at their institution, distributed from the content database according to the content owner's requirements. Distribution can take the form of online streaming, which allows no copying, or using an offline format, which allows the creation of a printed hard copy of the content or the saving of a personal copy as a file for offline use. A record of aggregated usage is reported to content owners and the participating institutions.

Educational institutions can be both the users and the content providers in this distribution system, but in general, the providers are digital media producers, including publishers, archives (e. g. the Canadian Music Centre), and museums. An important source of content for the OnDisC trial is the image database available through the Canadian Heritage Information Network. In addition to images, the media types to be tested in the prototype include music scores, video, music, photographs, animations, simulations, graphics, CD-ROM content and, of course, text.

Access to OnDisC is based on institutional licenses, similar to those used by AMICO or proposed by the National Site License Project, referenced in Section 2.5. These distributed digital content licensing agreements offer greater flexibility to both owners and users than sales contracts on individual items. License terms can be less onerous for users and better adapted to educational needs; at the same time, the content owner continues to receive intellectual property revenue and firmly controls the usage of the content.

The goal of the OnDisC project is to demonstrate that currently available technology can be used to produce an open distribution system, which combines

- creation and maintenance of content description (the catalogues),
- protected distribution to site-licensed users, and
- integration with a rights management system to provide reporting and accounting to providers.

3.3 Enforcing IP Rights Through Distribution Technology

Traditionally, distribution of content over the Internet has meant transferring a file from one computer to another—either through the venerable *ftp* service, or now, through an *http* (Web) server, in which case each file is a Web page, or element of a page. With either service, the content ends up as a stored copy in the file system of the receiving computer.

It is the existence of such copies which poses the main problem for the protection and management of the IP rights associated with digital content, accessed over a network. Once the content is available as a file in the local file system, under the user's control, there are no real restrictions on what the user can do with the file as a sequence of bits. Even if the content is encrypted, it can still be copied and transferred and inspected, as a data file.

However, there are approaches to content distribution which substantially reduce this problem, using a networked file-access protocol to make the user's operating system treat a portion of the server's file system as a part of the local file system (read-only, of course), so that files stored on server are opened remotely without being copied to a local disk (since to the user's computer, the file appears as a local file to begin with.) This is called "remote mounting", and in conjunction with a rights management system which controls access to the remote files, protects IP rights by avoiding the actual transfer of the content to storage on the user's disk.

Applications are, of course, very suitable for remote invocation since they are executed in memory, and do not normally leave a copy of themselves on disk in a form that can be easily recovered. Streamed video and audio files are also well-suited to protection through remote access, since special software —usually a 'plug-in'— is required on the user's computer to handle the data stream, which is only stored in memory. The streamed files are often much too large to be comfortably saved to the user's disk.

But what about *images*? These are neither executed nor generally streamed. If conventional browsers and graphic application are used to open them, even if remotely, they are vulnerable to the usual infringing operations by the user. The solution is to make the remote access only available through a special application, "plug-in" or applet which displays the image, and controls or restricts printing and copying. This doesn't completely prevent making local copies of the remote files, but it eliminates the possibility of casual copying and redistribution which are such persistent concerns for museums and archives.

3.3.1 Alchemedia and Vyoufirst

Rights management systems are commercially available with simpler functionality that the comprehensive systems described above, which are designed specifically for protecting images (typically, JPEG, GIF, and Acrobat PDF). A representative example is Alchemedia which provides:

- an encryption module that interacts with the provider's web server to encrypt requested files, prior to their transmission to a user's browser;

- a proprietary viewer which acts as a 'helper application' for the browser to view encrypted files and enforce usage restrictions;

- a remote management tool with which a content provider configures the configuration module on their web site.

A similar product is Vyoufirst™ from Vyou Inc., which however requires that the content provider install a special web server to serve the encrypted content. Vyou claims a broad range of controls over usage, including :

- blocking caching (creation of temporary copies on disk),

- prohibiting the use of debuggers (which access memory directly) to capture content,

- blocking clipboard operations, including third-party software which may operate independently of the functionality built-in to the operating system, and

- and blocking screen capture operations.

One difficulty with such claims is that it is very difficult to assess how successful the advertised controls are in actual practice. To determine the level of protection afforded by a product, one would have to know something about the mechanisms employed, and that is precisely the secret that security vendors must tightly guard if they are to avoid having the weaknesses in their products exposed and publicized by a hacker 'exploit'. Encryption (the staple technology) of such products, while adequate to prevent casual infringement, as are simple password and access codes, is far from a panacea for protecting valuable media, as shown by the wide-spread availability of software to defeat the encryption of commercial movies in DVD format. (An informal poll of a university computer science class showed that almost half of the students used such software.)

4 Protection Technologies

The protection technologies which we discuss in this report are :

- data embedding, in the form of:

  watermarking, both *visible* and *invisible*, which attempts to provide a unforgeable, unerasable identification of an image *source*, and

  fingerprinting to provide an unforgeable, unerasable identification of the *recipient* of an image copy;

- *encryption* to conceal the contents of a data object from an unlicensed user; and

- *container technology* to allow protected 'super-distribution' of data by any user whether licensed or not.

All these technologies are being used to one degree or another in rights management systems. We believe that *containers* incorporating *encryption* are likely to be the foundation of any comprehensive rights management system [Jurenka, 1997], but watermarking and data embedding lend themselves more easily to being marketed as discrete products with specific protections, and are hence likely to be more visible in the marketplace for image protection technologies.

4.1 Varieties of Watermarking

In a paper document, a watermark is a physical design embossed or pressed into the paper that can be seen when the page is held up to a light. In an electronic document, watermarks come in two forms: visible and invisible. A visible watermark is usually a faint background image superimposed on the document image, but if well done, it will appear to be "under" the image, as if the image on the screen were an image of an original printed on watermarked paper. Invisible watermarks are often not images at all but patternless arrangements of bits hidden in an image or sound file which are recovered from the file through a decoding application.

One function of a visible digital watermark is to make it apparent to a user that a document is *owned* and by whom. This is more easily and less intrusively accomplished with a copyright notice. But because the copyright notice appears only in one portion of the document, separated from the main body of the content, it will not appear in an excerpt such as a cropped image, so visible watermarks, like paper ones, are designed to be visible throughout a large portion of the image.

A visible watermark itself should be a fairly complex design to make forgery difficult. Unfortunately, the technology for imprinting watermarks into digital images can be readily obtained, and as programs can be written to accurately recover a watermark from a digital image, digital forgery can

be accomplished by any skilled person using a desktop computer. A standard but not necessarily effective way to counter this is to create an on-line "license" to which the user must agree in order to access an image, forbidding *any* alteration of the image. If taken literally, such agreements make a licensed image unusable for many legitimate purposes—for example, reducing the colour map to a grey-scale for monochrome printing is literally an alteration.

By specially designing the graphic used as a watermark, electronic watermarks can be created which are only visible when an image is printed, and do not appear on screen images. This technique has been used by the Picture Information Network (PNI) [Walter, 1995]. It is derived from techniques developed to block counterfeiting of financial documents using photocopiers or laser printers, and depends on particular features of the way today's copiers and printers are constructed.

Invisible watermarks are also intended to record the legal *source* of a document, (which may be the copyright owner), but in such a way to be undetectable by the user. This is essential for audio files and, in many cases, is highly desirable for images. At the same time, the watermark should be *robust* in a way that the usual copyright notice is not; the watermark should resist attempts to remove or degrade it and should survive transformations such as cropping or colour alteration for images, and the removal of silent intervals for audio files, so that the copy retains the watermark as evidence of ownership.

It should be noted that for some purposes, robustness, although a key concern in the research literature, may be of lesser importance for rights enforcement. If the ownership of the original of an image is clear, and the original is available as evidence, as in the case of images owned by a library or museum, then the distribution of a digital image with its watermark removed may *itself* provide legal evidence of a rights infringement. Articles 11 and 12 of the 1996 WIPO Copyright Treaty [WIPO, 1996] provide a framework in international law, which is being used as the basis for national laws (such as the US Digital Millennium Act) prohibiting the removal of rights-protection devices such as encryption and rights information, which includes object identifiers stored in watermarks.

4.1.1 Visible Watermarking

It is perhaps worth noting that embedding visible watermarks in images is not a difficult matter, from the point of view of the algorithms involved; implementing a reasonable watermarking scheme should be within the competence of a C programmer experienced in image formats and manipulation. Thus museums who wish to apply a visible watermark to a collection of images do not need to rely on proprietary software or third-party services; this is one area where museums can, if the need warrants, "roll their own".
When a watermark is *superimposed* on an image, it can interfere with its beauty. The effect might be interpreted as "doing violence" to, the image of a person's face, and thus might give offense to some members of the viewing public, or be viewed by the artist as an infringement of his/her moral rights. Another example, which could give offense, would be the marring of an image sacred to a particular religious group.

To avoid such negative effects, users can be required to use an image viewer with an option

allowing the watermark to be suppressed if a particular control-key is pressed when an image file is selected. This would seem to be a desirable feature in that the aesthetic, humanistic, or inspirational values of an image are thus preserved for the user. However, in order for options of this sort to be effective for users, special attention will have to be paid to educating users as to their existence and implications.

The choice of a watermark graphic must take into account many factors, if it is to succeed in achieving the desired effect when superimposed on images with a wide variety of pictorial and graphic qualities. It should be noted that a visible watermark may be easily removed using shareware graphic tools. The alteration can be done on a personal computer in a matter of a few minutes using commercially available image-manipulation software. As Digimarc's FAQ [Digimarc, n.d.] observes: "Since [a visible watermark] is visible and localized, removing a watermark is trivial. "

The problems with visible watermarks have made them less attractive as a protection methodology. IBM, which used visible digital watermarking in its early Vatican Library project, decided that it "was inappropriate for art; when darkly applied, it interferes with the visitor's experience of the art, and when lightly applied, it leaves the visitor wondering what is painting and what is watermark."[Mintzer, 2000] As a result, its Hermitage project relies only on invisible watermarking to protect the on-line high-resolution images.

4.1.2 Invisible Watermarking

Invisible watermarking is a branch of the growing discipline of "data hiding" or *steganography*. Multimedia objects, particularly sounds and images, inevitably contain bits which can be altered imperceptibly, and this can be exploited in many different ways to encode external information within the object, below the level of audible or visual detection. (In general, digital watermarks cannot be applied to simple computer-generated images or to ASCII text.)

In the case of visible watermarks, the information added to an image is intended to be seen, so that the source of the image can be recognized on inspection. For invisible watermarks, it is important that the added information *cannot* be detected by audible or visual inspection so that it cannot be removed, and the hidden data must not degrade the image, or only slightly reduce its quality. At the same time, it must be possible to detect and recover the watermark, using special software.

Invisible watermarking differs from encryption in that, through encryption, the object is made unusable; whereas the existence of the watermark should not interfere with the use of the object. The watermark is typically created and embedded using a secret key constructed by the originator and this key must be known in order to detect and decode the watermark in an image. Thus, it is usually the originator who does the verification, not the user. In some approaches, the original of the image must also be available for watermark detection.

Watermarks which are detectable without access to the original content are amenable to the enforcement technique of using a software "robot", or just "bot" (also called a "spider" [Cheong, 1996]), to crawl over the Web from one site to another, looking for files which contain a specific

watermark. Such a "bot" can provide a very inexpensive way of collecting data identifying the sources and degree of infringement, on a global basis.

> Images are routinely transformed by being compressed for distribution, scaled, or by being cropped. Therefore, watermarking techniques must be robust enough to survive, at a minimum, both compression and geometric transformations.

It is also desirable that the watermark be distributed throughout the image so that its existence can be detected from a portion of the original. Ideally, the watermark should also survive printing, so that if the printed image is re-digitized through scanning, the watermark can be detected [Cox, I., 1996].

An important feature of watermarking, as compared with other protection techniques such as encryption, is that it alone can provide protection for audio and video media even when they are converted from the digital to the analogue domain; the watermark can, if properly constructed, be recovered even from an audiotape or videotape made by recording the output from speakers or a screen, or intercepting the electronic signal from a sound card or a video output of a computer.

The primary use of invisible watermarking, like that of visible watermarks, is to provide owners of copyrighted content with the means to prove their ownership from the data stored in the content, and to provide evidence of copyright infringement. Unlike a visible watermark or copyright notice, the invisible watermark is typically different for each image. It can contain a work identifier, a time-stamp, copyright information, information about allowed uses, etc., within the limits of the allowed size of the watermark (usually no more than a few thousand bits, or a few hundred characters).

As with cryptography, the techniques for invisible watermarking, and steganography in general, involve the application of sophisticated mathematical ideas, but their development requires no special equipment or software. As a result, this field is very well-suited to academic research, and with the emergence of a commercial market for watermarking products stimulating research efforts, a wide variety of watermarking algorithms have been proposed in the research literature. Useful pointers to current work in this area are found at the sites maintained by Hartung and Peticolas. [Hartung, 1997; Petitcolas, 2000] A detailed summary of the various roles and requirements for watermarking is given in [Voyatzis, 1999].

One stimulus for such research has been the vulnerability of some initial watermarking schemes. Identification of possible attacks and proposals to meet them has been a staple of the watermarking literature. Contributing to some skepticism about the actual protection provided is the fact that commercial watermark algorithms are secret, although likely based on published research. In the related field of cryptography, it has long been recognized that secret algorithms are not as trustworthy as published ones which can be analyzed, subjected to experimental attack and improved, based on the expert community's experience with the algorithm (See [Schneier, 2000], for a lively non-technical discussion.) Secret algorithms can be defeated—the secret can be stolen or uncovered, but they do not have the possibility of improvement through analysis and challenge. This has motivated the development of the StirMark benchmark [Kutter, 1999; Petitcolas, 1999] for watermarking products, to provide an independent rating scheme, using open techniques which can be easily reproduced by others, rather than relying on irreproducible claims by vendors.

As in cryptography, an "arms race" scenario is likely, in which the vendors attempt to incrementally improve their products to deal with each new challenge, while the expert community continues to probe for and publish weakness. In the near term, it is likely that there will be both defeats and successes on either side, with the corollary that the technology will continue to evolve and improve.

4.1.3 DCT-based Watermarking

Watermarking algorithms commonly work in the *spatial domain* of the images; that is, they identify appropriate locations in the image that are then altered to incorporate the added information. A problem with such methods is their lack of robustness in preserving the watermark after image transformations. An alternative approach involves representing the image in the 2-dimensional *frequency domain* (analogous to the 1-dimensional analysis of an acoustic signal in terms of frequencies rather than amplitudes), using the Discrete Cosine Transformation (DCT). (This transformation is the basis of the widely-used JPEG compression algorithm for images.) The watermark is added to the image by manipulating the frequency coefficients in the DCT and the resulting frequency representation of the image is converted back to the spatial domain using the inverse transformation to the DCT. The DCT approach is combined with the spatial approach by determining specific regions to which a DCT-based method is applied, either pseudo-randomly as in the algorithm used by SysCoP, or using criteria such as noise-sensitivity.

Cappellini and his group at the University of Florence [Barni, 1998] have developed a sophisticated form of DCT-based watermarking which does not require the original image for detection, and which has been demonstrated to be quite robust against a wide variety of attacks, including:

- geometric distortions (resizing, cropping, etc.),
- JPEG compression,
- low-pass filtering,
- median filtering,
- line inversion, and
- insertion of additional watermarks.

4.1.4 Tracking the User

An alternative or supplement to digital watermarking as a deterrent to copying or alteration is the embedding of usage information in the document itself. This has been called *digital fingerprinting*—the creation of an invisible record of user information, based on information collected at the time the distribution of the image to the user was authorized. If the document thereafter appears in a context which suggests it was illegally copied or transferred, the identification of the user initially responsible for the rights or license violation can be recovered. As with digital signatures, the degree to which electronic documents can be fingerprinted depends on the content and is easiest for document types that have a large number of bits and a "noise level" such as real-world images and sounds.

The same sort of steganographic techniques used to create invisible watermarks can also be used to implement digital fingerprinting. With a hidden transaction history housed in the user's copy of the digital content, which can be altered or removed only with great difficulty, it is argued that

honest users will be deterred "from doing dishonest things. Users will be less likely to abuse tracks if they know their fingerprints are in the music" [Cognicity, 2000].

4.2 Encryption

Digital encryption refers to the process of mathematically transforming a data object so that it can only be "read" or made use of by someone who possesses a specific secret piece of information: the decryption key, which is used to reverse the mathematical transformation and recover the original data.

Encryption serves a variety of purposes in the context of delivering copyrighted or licensed information over a network:

- It prevents "theft" *en route*. At present, most networks, and especially the Internet, are insecure. The data travels through many "hosts" between sender and recipient, and these hosts can, in principle, detect and collect the information as it flows through. (For this reason, passwords, credit card numbers, and similar identifiers should never be transmitted over the Internet without encryption or other security measures.)

- It can be used to require that the recipient perform an additional transaction, such as obtaining a "password" or decryption key, in order to decrypt and view the material. This is the approach often taken by vendors of CD-ROMs containing collections of fonts or games. A similar approach requires the user to enter a password of their own choosing for authentication purposes, which then automatically triggers the transmission of the decryption key to an application on the user's machine. (This is the approach used for secure transmission of user data to a website.)

- The user may be required to use special software, which, while decrypting and displaying the content, does not allow the user to use normal operating system functions such as file copying or copy-and-paste operations, thereby protecting the content, to some extent, from user modifications and re-distribution to others.

Traditional encryption techniques use the same key for both encryption and decryption; thus both sender and recipient have to *share* a secret. This poses great difficulties in the context of distributing content over a telecommunications network, where sender and recipient cannot easily meet face-to-face for the secure transmittal of the key, and where senders cannot be sure recipients will keep the secret with which they have been entrusted.

The technical innovation known as *public-key encryption* [Fahn, 1993] has been responsible for making encryption a practical tool for protecting digital content. In public-key encryption, an individual generates a pair of keys in the form of long numbers or character strings (typically using a computer program)—a public key, which is published or made available to anyone who wishes to send an encrypted message to the person who generated the public key, and a private key which is kept secret so that only the person who generated it can use it to decrypt a message. The public-private key pair has a special mathematical relationship, such that messages encrypted with the

public key can be decrypted using the private key. A simplified example of how it works, using the stock characters of the encryption literature, Alice and Bob:

> Suppose Alice wants to send Bob a secret message which only Bob can read. Alice looks up or asks Bob for his *public key*. (a long string of apparently random characters). It's not secret, so Bob can send it to her by e-mail or Alice can get it from his Web page. Alice plugs the key into her encryption software and types in her message. Out comes an uninterpretable file of apparently random characters, which she sends off to Bob. Bob uses his encryption software into which he has entered his private keys to read the message.

The key point: Alice and Bob did not have to share any secret in order for this to work.

In practice, only very short messages are encrypted using public-key encryption, as the method is computationally intensive. A common method of applying public-key encryption to the encryption of digital messages is to use a public key to encrypt *another key* to be used in a secret-key method such as the widely used Data Encryption Standard (DES). The sender encrypts the actual message using this secret key, and the receiver decrypts the message using the same key which the receiver decrypted using his or her private key.

DES encryption and decryption software is widely available and is substantially faster than public-key algorithms. It can be applied to images by dividing the image up into blocks of, say, 64 bytes; each block is encrypted and decrypted using a 64-byte key which scrambles or descrambles the contents of each block.

Here's a simplified example of how this might work in the transmission of an image from an image database (called Alice) to a user called Bob:

> Bob selects an image to be viewed from a list presented by a browser. The browser transmits the request to the Alice server, and includes a public key to be used just for this transaction. (The public key is not a secret and so can be transmitted over an insecure Internet connection.) The Alice server encrypts a DES key (to be used just for this transaction) with Bob's browser's public key and sends the encrypted key back to Bob. This is quite safe because if the key were intercepted in transmission, it couldn't be used without access to Bob's browser's private key. Alice then encrypts the selected image with the DES key and transmits the encrypted blocks to Bob's browser, which uses the DES key it has received to decrypt and display the image.

Notice that in this scenario, the user is not involved in any aspect of the cryptographic rituals being carried out by the software.

4.2.1 Signatures for Authentication

Public-key encryption can be used for *authentication* of the source of a document (image, etc.) by verifying mathematically that an entity claiming to be the source has access to the secret private key that corresponds to the source's public key. The procedure (somewhat simplified) is as follows:

> Suppose Bob wants to know if the encrypted message received from Alice really comes from her. Since Alice used Bob's public key for the encryption, Bob uses his secret private key to decrypt the message, yielding as part of the message, a "signature" which Alice had

encrypted with her private key. The "signature" is not something peculiar to Alice, such as her handwritten signature, but is a quantity depending on the *message*. It is a fixed-length number that has been computed from the message, with the property that it is infeasible for anyone to determine what messages could have yielded that signature value. But Bob has access to the message itself; he has just decrypted it. So he can apply the "signing procedure" (if he didn't know which one to use, Alice could have told him in her message) to the message and see if he gets the "signature". If so, the message could only have come from someone with access to Alice's private key, presumably Alice.

While authentication is an important aspect of public-key encryption, it is not as relevant in the domain of digital image distribution. There, a different concept, which also goes under the name of *digital signatures*, is used, which we discuss in section 4.3.

4.2.2 Software vs. Hardware

Distributors of images typically secure the contents of image files through proprietary file formats and encryptions which require the user to obtain a special viewer program in order to decrypt an image. The viewer program must therefore share a secret (the decryption method or key) with the content provider, who must hope that the user will not attempt to discover it, by for example, analyzing the code in the viewer. Additionally, the content provider must assume that the user will have a strong interest in the content to voluntarily download the viewer, or accept an automatic download. But, requiring users to install special viewer programs or plug-ins for each separate commercial encryption technology is a doubtful proposition, unless a single technology comes to dominate the market or standards are imposed.

One form which such a standard may take is indicated by the IBM/4C protection scheme [Lehmann-Haupt, 2000], which relies on a significantly new approach—the content is encrypted in such a way that it can only be decrypted by compliant *storage and playback devices*. The initial application is to create MP3 players which will only play permitted copies, but the concept is extensible to hard drives and hence to the control of image copying at the hardware level in the user's PC. IBM and other manufacturers already have standards for disk drives along these lines. [Orlowski, 2001] Some details on the issues relating to hard-drive-embedded copy protection are provided in [Schneier, 2001].

It is unclear at this point whether vendor organizations in cooperation with content providers will be able to enforce encryption at the hardware level throughout the consumer computer market, but if they are successful, the legal sanctions against circumvention and tampering will likely make attacks more costly, and the current forms of infringement through copying for convenience or for sharing may become greatly reduced, although not completely extinguished, as has happened in other areas such as cable descrambling.

4.2.3 Defeating Encryption at the Software Level

If a distributor of encrypted images requires a special viewer or plug-in for decryption, it is desirable that the file be formatted in some standard way (say, as a JPEG file) so that it can be easily downloaded using a browser such as Netscape or Internet Explorer. The file then exists on the

user's hard drive (for example, in the Web browser's "cache" of downloaded Web files), but appears to be empty to the usual JPEG viewing software due to the encryption. The application or plug-in which allows the user to view the image will typically not allow copying or printing, and since the browser is not handling the display, its print and copy commands are inoperative for the image window. However, this may not preclude the user from quite easily copying and manipulating the image. With a few key-presses, the entire screen, including the display produced by the viewer software, can be easily captured in a file in a standard (unencrypted) format.

This is possible because the image is necessarily available in memory in an unencrypted form for the purposes of display, and the operating system command that captures a screen as a file has not been disabled. Even if the viewer application (such as the Vyoufirst client) disables screen capture temporarily, this will not necessarily prevent copying of the unencrypted content, for it is quite feasible to write a program which, when activated, does what the screen-capture command would have done, finding and copying the image data from memory to a file.

If the user is using "virtual memory" to extend the memory space of his or her computer, then the decrypted content created in memory from an encrypted document may at some point be transferred by the operating system to the part of a hard drive being used to as an extension of memory (the "swap space"), where it easily captured using standard disk tools, even though it was never explicitly stored as a file. A number of popular data encryption products are vulnerable to attacks of this sort. [Rowan, 1997]

4.2.4 Interaction Between Compression and Encryption

Compression reduces the redundancy or patterning in a file and this aids encryption by reducing the redundancy of the file. In addition, the compression scheme shortens the data file, which reduces the amount of work needed by the computer to execute the encryption algorithm. Thus a fast compression algorithm enhances security and improves the performance of an encryption algorithm.

If compression algorithms such as JPEG and encryption algorithms such as DES are used, compression should never follow encryption. A good encryption algorithm will produce output which is statistically indistinguishable from random numbers, and compression algorithms cannot reduce the size of a file of random numbers (the JPEG algorithm may actually *increase* the size.)

However, there are disadvantages of applying DES-style encryption to compressed images, as outlined by Macq and Quisquater [Macq, 1994]:

- An originator may wish to protect his images independently from the transmission process, thus independent of the compression algorithm used, and prior to transmission.

- Compression techniques are very sensitive to transmission errors and are protected against errors by adding additional framing and synchronization data. This data must be exempted from encryption, which weakens the encryption, or must be omitted, which increases the chance of a transmission error.

- In many applications, the encryption should be partially transparent; for example, "thumbnails" or "previews" stored as part of the image file should be left unencrypted or partially encrypted (compare the TIE system described below.)

For these reasons, Macq and Quisquater [Macq, 1994] have proposed an image encryption technique in which encryption can precede compression. They propose a multi-resolution scheme that produces a compressible image with a given level of transparency.

The encryption process encodes only the details above a given resolution, and produces an encrypted image that has similar statistical properties to unencrypted pictures, so that it is compressible.

4.3 Data Embedding Technologies

In this section, we briefly examine three commercially available protection technologies which use digital watermarking and, more generally, hidden data embedded in the digital content. (Contact information for the vendors of the products mentioned is found in the Vendors and Organizations section of this report.)

4.3.1 Cognicity

Cognicity offers a watermarking tool, Audio Key™, which embeds data in an audio, image or video host signal without affecting the quality of the content. This watermarking is very robust and maintains its integrity even when the original is edited, compressed or translated between formats. Cognicity claims that the security watermark will persist even when the digital content is converted into an analog format.

The AudioKey product also comes in an industrial strength version, AudioKey Pro, which can also embed access restrictions for digital content to specific users for a defined time period.

AudioKey can be paired with another Cognicity product, Audio Key MP3™, which embeds information about the transactional history of the digital content directly into the content. The record begins with the initial transaction; the record can include information about the content owner, content identification information, vendor information, and the transaction information. This record provides information to the content owner to easily identify both the true ownership and also any 'sharing' or pirating of the content during its life-span.

4.3.2 Digimarc

Digimarc Corp. offers a widely publicized technology for embedding information such as electronic signatures or other information directly within photographs, video, audio, and other creative properties which are based on "real-world data". It does not apply to computer-generated images or to ASCII text.

Digimarc watermarks (previously called "signatures") are created by combining an apparently random code unique to the originator with the information to be embedded in the data. The watermark can be added to an image using a "plug-in" in conjunction with image-manipulation software, such as Adobe Photoshop. A Digimarc watermark cannot be added to a digital image that already contains watermarking.

The watermark is then added to the digitized image (or other creative property) at a signal level below the level of the "noise" or randomness inherent in image or sound data. This makes the watermark invisible to the viewer but it is easily recoverable using the creator's unique code pattern, and cannot be detected or removed without access to the code. The Digimarc watermark is distributed throughout the image, so that subsequent modifications can be identified, such as in photo-ID cards.

The technology is marketed as a means of reassuring creators that they will be able to prove copyright or license violations, rather than preventing them. A "spider", *MarcSpider*™, is available to search the Web for usages of Digimarc-watermarked images. Tracking digital content with the *MarcSpider* is provided by Digimarc on a subscription basis to clients. The subscriber receives Web-based reports of digital content usage during the subscription period.

The tracking service uses the major search engines on the web to find the watermarked material in use. This service has a downside – the spider can only find instances of the images' use on the web if the site has previously been indexed. Digimarc offers a *MarcSpider* disclaimer on their webpage:

> "This means that MarcSpider is not likely to find all your watermarked images, particularly when they appear on sites that are not very heavily indexed by the major directories and search engines."[Digimarc]

Digimarc claims a wide range of uses for its technology: besides providing simple proof of ownership, signatures can contain other digital information such as

- license rights,
- usage rules and restrictions,
- creation data, including camera data,
- distribution path,
- contact information for rights management systems, and
- content identification such as captions or adult content warnings.

In comparison with other copyright-protection mechanisms, Digimarc argues that invisible watermarks can identify ownership and other information about an image or other intellectual property without completely locking out access (such as encryption does), being separable from the image (as the file headers may be) or damaging the image (as watermarking, thumbnails, or reduced resolution versions do).

4.3.3 MediaSec

SysCoP (System for Copyright Protection) was developed at Fraunhofer Institute for Computer Graphics (Darmstadt, Germany) by J. Zhao, and is now marketed by MediaSec Technologies. As in the Cognicity and Digimarc approaches, the embedded data is claimed to be invisible, unremovable and resistant to damage through compression or changes to the file format.

MediaSec lists the following typical categories of embedded information:

- copyright,
- origin and owner,
- destination or transaction,
- usage rights, and
- document characteristics.

SysCoP supports several types of watermarks:

- hierarchical watermarking embeds multiple information sets into one multimedia document in such a way that each can be extracted independently, in order to track and identify a multimedia copyright transaction chain;

- regional watermarking embeds a label within or outside a specific region of multimedia data;

- public watermarking embeds information that can be read without a secret key.

It is claimed that the embedded information is robust against lossy compression (such as JPEG), format conversions, low-pass filtering, color reduction, printing or scanning, rotating, scaling, and cropping.

SysCoP supports still image, motion data, and document formats as summarized in the following table:

Media type	Supported formats
Image	PPM, PGM, GIF, TIFF
Video	MPEG-1, MPEG-2
Formatted page images	Postscript

Different media require somewhat different methods, but they all share two basic steps: the first step is to generate a sequence of pseudo-random positions where the data is to be embedded, using extracted image data together with a user-supplied secret key supplied by the content provider as the seeds or starting values for the pseudo-random number generator. The second step simply embeds or retrieves the code into or from the locations specified in the position sequence.

It is noteworthy that while most embedded data technologies are designed to work only with "natural" images (or audio), SysCoP methods are applicable to text.

The TIE project at the Fraunhofer Institute, Darmstadt, developed an experimental server for images with *encrypted regions*, which allows the image to be partially viewed without special software beyond the user's browser. This technique of selective encryption is now available commercially from MediaSec in the form of the MediaCrypt™ product, in which original data in the scrambled regions is appended to the image file and transmitted in an encrypted form.

4.4 Secure Container Technologies

Containers are software components that can contain a variety of different media objects; when accessed by a user, the container activates appropriate processes such as decryption, viewing, etc. The container is not an inert object such as a data file that can be opened and manipulated by a wide variety of applications; it incorporates code as well as data and only allows itself to be read or altered under specific conditions.

Container technologies are themselves based on the concepts found in *software component architectures* such as Microsoft OLE and Sun Microsystems JavaBeans, and provide the basis for secure distribution of media through rights management systems.

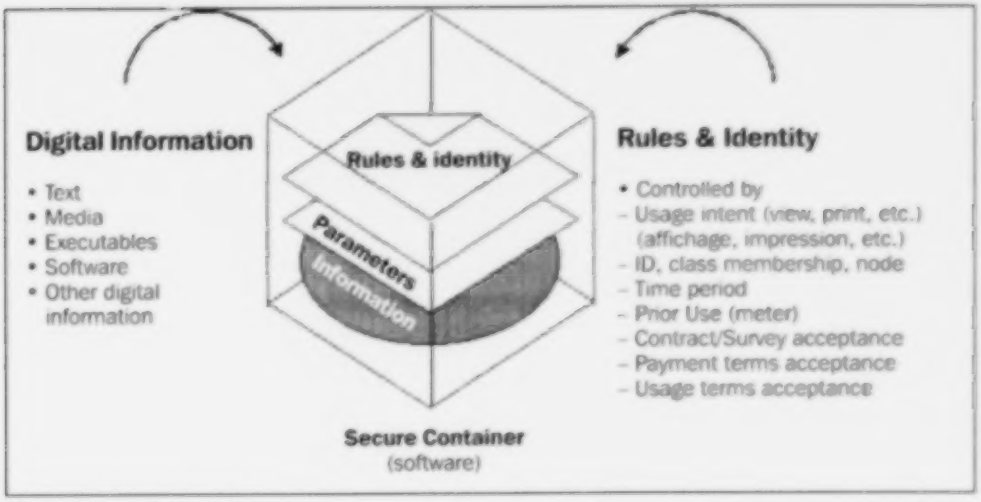
We present a snapshot of two currently available container technologies: InterTrust's *DigiBoxes* and RightsMarket's *RightsPublish* products, to show the similarities and general convergence of concepts.

4.4.1 InterTrust's *DigiBoxes*

InterTrust licenses its technology to partners and application developers. A key component is the *DigiBox*™ container technology, which provides a way of securely encapsulating content to be managed and protected by the InterTrust rights management system. Software developers can write applications such as servers, browsers and "plug-ins" which implement the DigiBox model by including code from software libraries provided by InterTrust. Data relevant to rights management, such as price and license information, are embedded in the container along with the content data — images and text.

Security is provided by encryption throughout: it is used to prevent unauthorized access to the content of DigiBox containers, to protect the rights management components from tampering with critical business information, and to ensure the privacy of users with respect to usage data.

Information housed in a DigiBox container remains protected even after a user has accessed it or while the container is travelling across unsecured networks. Content usage rules can also be stored in the container, travelling with the information, or could travel separately, to allow for rule flexibility after the content has been delivered:



Digibox secure container.

4.4.2 RightsMarket *RightsPublish*

RightsMarket provides an "end-to-end" digital publishing technology that can be integrated with an existing publishing website. The digital content is encrypted and wrapped into a container which interacts with a RightsMarket application on the user machine and a media player/reader for the particular file format of the content. (Currently supported formats are Acrobat's PDF for page image files and WinAmp mp3 audio files. By supporting PDF, RightsMarket's technology also accommodates a full range of image types, either as single images or as collections.)

A *RightsPublish* container (referred to as a "digital property") has a number of interesting features:

- The encryption is persistent. Content is decrypted only during authorized use and the decrypted content is not saved;

- To obtain a digital property and authorization to use it, the user uses an Internet connection to access a RightsPublish server, which downloads the property to the user's hard drive. When the user wishes to open the property, the RightsMarket application on the user's machine verifies that the user is authorized to do so, and enforces the terms of use. Thereafter, if the terms of use allow it, the user can use the property in offline mode; there is no need to reconnect for each use. If the property is acquired on a pay-per-use basis, the offline usage may be limited to a certain number of 'plays', which are logged with the RightsPublish server the next time the user establishes an Internet connection;

- If a user loses purchased digital properties or wishes to access purchased properties from a different machine, they can, if allowed by the license, download another copy;

- RightsMarket implements true "super-distribution", in that users may freely copy or distribute the objects they have downloaded, but such copies cannot be further used by users who have not obtained authorization via the RightsPublish server.

The RightsPublish model is currently directed to support 'retail' digital publishing, in which users license the usage of digital objects as individuals, and pay for that usage on a per-use or per-time basis. But it may be adaptable to other markets that involve broader licensing to educational institutions, as in the OnDisC model described in section 3.2.4.

5 On the Horizon

The technologies described in the last chapter are understandably conservative and defensive, but the development of multimedia and its distribution continues at a very rapid pace, enabling new applications and patterns of use which could hardly have been foreseen even a few years ago. In this concluding chapter, we look briefly at three rather different examples of newly emerging technology likely to have some substantial impact on how digital images are presented and protected. In each case, although the specific focus of the technologies is not on intellectual property or rights management, it is evident that IP issues are now being taken explicitly into account in the early stages of specification and development. This marks a departure from the typical path of technical innovation in previous years, where (as in the case of the standardization of CD-ROMs) IP was not considered until well after the technology had become widely used.

The examples represent three distinct facets of what we can anticipate for the media of the near future:

- the increasing standardization of methods for describing digital objects, enabling more useful catalogues and search functions;
- the development of more elaborate and more powerful methods for compression of images, making it practical to transmit larger, higher resolution, and more complex images;
- the specification of standard components in the creation of new forms of interactive presentations, through the integration and composition of varied types of media streams.

5.1 Rights Metadata and XML

The distribution of images and digital objects in general requires the distribution of information about those objects as well, so that users can make selections and understand the nature and context of what they are viewing. This *information about information*, similar to the catalogue information in traditional libraries, is termed *metadata*. Metadata is as varied as the data which it is about, but a highly flexible and expressive standard syntax for metadata has recently emerged - the *eXtensible Markup Language* (XML). Like its sibling, *HyperText Markup Language* (HTML), and its parent, *Standard Generalized Markup Language* (SGML), it uses tags surrounding text fragments as in

```
<format>audio/mpeg
    <extent>8 MB</extent>
    <duration>0:07:01</duration>
</format>
```

but in XML, the tags are not fixed by the standard, with significance only for the creators of the markup; they can be freely invented for specific contexts or applications, to reflect concepts which are meaningful to users. The mixture of standardization in syntax and freedom in semantics facilitates the automation of information exchange between different systems and computing

platforms, while preserving the concepts that are meaningful for a specific community. In the museum community, the CIMI consortium has participated in developing a set of tags which builds on established museum documentation standards, and on an earlier work on metadata elements by the various content communities, known as the Dublin Core. [Degenhart Drenth, 2001]

For rights metadata, Dublin Core provides a single <rights> element which is to be used to encode rights information, leaving it open as to how this should be implemented in specific situations. This can be as simple as indicating who has the rights and who has licensed access to the object:

```
<rights>
    <licensor>Encyclopedia of Music in Canada</licensor>
    <licensee>Sheridan College</licensee>
    <licensee>Canadian Film Centre</licensee>
</rights>
```

or it can be much more elaborate, including detailed descriptions of the conditions of use.

As a contrast to the previous very simple example, here is a small excerpt from a much more complicated example of the description of a work and its usage rights, as given by ContentGuard in its specification for an extensible rights-management markup language (XrML) based on XML. [ContentGuard, 2000] The example describes an electronic book containing an image with a time-limited license to access and view it on a specific device:

```
<XrML>
. . .
<OBJECT type="BOOK-LIT-FORMAT"> <ID type="ISBN">8374-39384-38472</ID>
<NAME>A book of James</NAME>
</OBJECT>
        <AUTHOR>James the first</AUTHOR>
<PARTS><WORK>. . . <OBJECT type="Image"><ID type="relative">1</ID>
<NAME>Image 1: Photon Celebshots Dogs</NAME>
</OBJECT></WORK></PARTS>. . .
<RIGHTSGROUP name="Main Rights">
<DESCRIPTION>Rights granted to John Doe</DESCRIPTION>
<BUNDLE><TIME><FROM>2000-01-27T15:30</FROM><UNTIL>2000-01-27T15:30</
UNTIL>
</TIME>
<ACCESS><RIGHTSLIST><VIEW><ACCESS></RIGHTSLIST>
. . .
<OBJECT type="MS Ebook Device"><ID type="INTEL SN">Intel PII 92840-AA9-39849-00</
ID>
<NAME>Johns Computer</NAME></OBJECT>
</RIGHTSGROUP> . . .
    </XrML>
```

It is an open question whether the highly detailed and logically intricate style of rights metadata proposed by ContentGuard will lead to an accepted standard (competitors exist, such as TrustData's proprietary RightsXML™ language), but in any event, the scope and depth of the XrML specification indicates the growing interest in being able to represent complex license data and use rights within an object's metadata in a uniform non-proprietary fashion. To the extent that this facilitates the rights management process through the development of applications that can enforce and track licensed usage, rights metadata is likely to enable wider distribution of licensed objects.

5.2 JPEG2000

Much of the image compression technology which we currently use, such as the well-known JPEG compression algorithm, has traditional mathematical roots associated with such famous names as Newton and Fourier. But on the horizon is a new and significantly more powerful algorithm dubbed *JPEG2000*, based in part on the refreshingly recent mathematics of *wavelets*. In both the JPEG and JPEG2000 algorithms, the compressed representation of an image is given in terms of a complex combination of mathematical functions which selectively capture different aspects of the image, and, in the case of *lossy* compression, omit features which are not visually detectable. In the currently used JPEG algorithm, these functions are trigonometric, capturing information about spatial frequencies. In the case of wavelet compression, the functions used to compress the image data are much complex; rather than being continuous "tones" of fixed frequencies, as in the 'one size fits all' approach used in the digital cosine transformations (DCT) of the current JPEG algorithm, the wavelet functions have specific shapes selected to efficiently represent the varying levels and types of details found in the image [Johnson, 1999]. (In 1988, Ingrid Daubechies, a mathematician working at Bell Laboratories, found a series of such functions which have become the basis of practical wavelet technology.)

The new technology requires decoders that will be significantly more complicated (and hence require more processing power) than current JPEG decoders, but it has a number of advantages [Christopulos, 2000] that are significant for digital image distribution, among them:

- high quality image and fidelity in colour image processing, with greater bit-depth and image size,
- greater flexibility in compression quality ranging from lossless to very high compression ratios,
- variable resolution, allowing regions with significant details to be encoded at higher resolution (Region Of Interest (ROI) coding),
- variable encryption, applied to selected parts of the image,
- image files composed from multiple components of different bit-depth encoded with different compression transformations,
- the use of special algorithms to compress text portions of an image to prevent the compression from introducing small inaccuracies that would interfere with accurate optical character recognition (OCR),
- explicit provision for metadata, including digital rights management data, embedded in the image file.

The JPEG2000 features pertaining to encryption and metadata reflect a growing recognition that a defect of earlier standards for encoding digital media was their failure to provide explicitly for the inclusion of metadata and the protection of the content. Publishers and distributors of digital content can now have some confidence that the new generation of more powerful standards will include the structures needed for proper description of the content, both contextual and technical, and the identification of the object and its permitted uses.

What will be the impact of JPEG2000 on watermarking technology? This is a topic of active research; initial results suggest that images can be invisibly watermarked in the "wavelet domain" [Santa Cruz, 2001], with greater robustness than conventional watermarking, suggesting that watermarking can be fairly easily integrated into JPEG2000 technology, which should increase its general usage as a protection technique.

5.3 MPEG-4

MPEG-4 is an ISO/IEC standard for multimedia, developed through the same process leading to the widely used compression standards for video, MPEG-1 and MPEG-2. But MPEG-4 provides a much more comprehensive and detailed view of the structure of multimedia than the previous video standards that were restricted to single bit streams combining video and audio. In MPEG-4, the goal is much more ambitious—to enable the integration of the production, distribution and content access paradigms of the three broad areas which are thought to be crucial for the future of multimedia: digital television, synthesized graphic content such as animations and modelling, and interactive multimedia, distributed over the World Wide Web.

Standardized methods are specified in MPEG-4 which can be used to:

- represent units of aural, visual or audiovisual content, called "media objects". These media objects can be of natural or synthetic origin; they could be recorded with a camera or microphone, or generated with a computer;

- describe the composition of these objects to create compound media objects forming complex audiovisual scenes, while still preserving the identity and structure of the individual objects;

- combine and synchronize the data associated with media objects, for efficient transport over a digital network ; and

- provide for user interaction with the audiovisual scene generated at the receiver's end.

It is noteworthy that MPEG-4 wholeheartedly embraces the "object-oriented paradigm" for media objects, a paradigm that has been enormously influential in the efficient production of complex software, and that underpins the concept of components and containers described earlier.

MPEG-4 enables the production of content with far greater reusability, and greater flexibility than is possible today with the current separation of media into distinct technologies such as video, graphics, and World Wide Web (WWW) pages. As well, MPEG-4 brings higher levels of interaction to end users, and enables multimedia for new kinds of networks, including networks with very low bit-rates, such as wireless and mobile communications. For these reasons, MPEG-4 is likely to be of significant interest to museums who are creating virtual exhibits and integrating digital materials from multiple sources.

However, the increased complexity of the media objects and the varieties of interaction on the part of the user definable within MPEG-4 also greatly increases the problems of managing the rights associated with the objects and their uses. MPEG-4's contribution to rights management is twofold:

(1) The standard specifies a consistent structure for the "hooks" within MPEG-4 compliant applications to proprietary rights management systems which use encryption and embedded IP data such as watermarks. With this interface, proprietary control systems can be easily amalgamated with the standardized part of the MPEG-4 decoder. This should make MPEG-4 technology more attractive to content owners, thereby contributing to the wider availability of the richness in the integrated interactive digital media which it enables.

(2) Each audio or visual object has a descriptor containing a data field for the persistent identification of intellectual property (IP), enabling the current holder of the rights to the object to be identifiable by accessing appropriate industry databases. Identifiers are likely to be those issued in international systems such as the International Standard Audio-Visual Number, which plays the same role for audiovisual material which the International Standard Book Number (ISBN) plays in the book publishing business. If a standard identifier is not available, the IP can be identified by metadata elements such as those given in the examples in Section 5.1

But the problem of maintaining the persistence of such an identifier, which is already difficult for MPEG-2 video streams, is reinforced in MPEG-4 due to the wide range of interactions and transformations of the media that are defined within the standard. (See, for example, the doubts raised by Henri Maître [1998].) The MIRADOR (MPEG-4 Intellectual Property Rights by Adducing and Ordering) project, within the EU Advanced Communication Technologies and Services (ACTS) programme, has the objective of developing appropriate watermarking algorithms which survive under these operations, and designing adequate countermeasures for a variety of attacks specific to MPEG-4. [MIRADOR, 1999]

Sources

ALA, "Digital Millennium Copyright Act, Section 1201(a) Rule", January 2001
http://www.ala.org/washoff/Rulemaking.PDF

Alchemedia Technologies, "Frequently Asked Questions"
http://www.alchemedia.com/products/faq.html

Alsford, S., "The Canadian Museum of Civilization Stakes Out a Site in Cyberspace", Museum Management and Curatorship, *13 (4), Dec. 1994, pp. 420-422. See:*
http://www.civilisations.ca/membrs/lobby.html

"American Memory", Library of Congress
http://memory.loc.gov/ammem/amhome.html

AMICO, "AMICO Library University Agreement", June 1998
http://www.amico.org/docs.html
http://www.amico.org/docs/AMICO.Univ.Agrmt.pdf

AMICO, "Frequently Asked Questions (FAQ)", Version 1.3, n. d.
http://www.amico.org/faq.html

Anderson, R. J. and F. A. P. Petitcolas, "Information Hiding: An Annotated Bibliography"
http://www.cl.com.ac.uk/~fapp2/steganography/bibliography.html

Arthur, Charles, "Digital Fingerprints Protect Artwork", *New Scientist* 144 (12 November) 1994. p. 24.

Barni, M., Bartolini, F., Cappellini, and A. Piva, "Copyright protection of digital images by embedded unperceivable marks" *Image and Vision Computing*, 16, 1998. pp. 897-906.

Baldazo, R., "Virtual CDs on the LAN", *Byte*, December 1995. p. 153.

Besser, H., and A. Richeson, "Protection—Watermarks, Fingerprints, Signatures", 1996
http://www.sims.berkeley.edu/courses/is290-1/f96/watermark.html

Bridgeman Art Library, "What is copyright?", March, 1999.
http://www.bridgeman.co.uk/public/copyrights/index.jhtml?r=7203

Bridgeman Art Library, n. d. "Copyright Warning",
http://www.bridgeman.co.uk/

Busch, Joseph, "SGML for Cultural Heritage Information", 1995.

Canadian Heritage Information Network, Sample CD-ROM Licensing Agreements for Museums, Quebec Civil Law Edition, 1997, Canadian Common Law Edition 1997, *Public Works and Government Services Canada, 1997.*

Canadian Heritage Information Network, "Capture your Collections' Digitization Course, 2001.
http://www.chin.gc.ca/English/Digital_Content/Managers_Guide/index.html

Cheong, Fah-Chun, Internet Agents, Spiders, Wanderers, Brokers, and Bots, *New Riders: 1996.*

Christopoulos, C. A., T. Ebrahimi and A. N. Skodras , "JPEG2000: The New Still Picture Compression Standard", *Proceedings on ACM multimedia 2000 workshops*, 2000. pp. 45 – 49.
http://woodworm.cs.uml.edu/~rprice/ep/christopoulos/

Clark, Richard, "An Introduction to JPEG 2000 and Watermarking", Secure Images and Image Authentication Seminar, Professional Group 4E, IEE Symposium. April 10, 2000.
http://www.jpeg.org/JPEG2000.htm

Cleveland, Harland "The Twilight of Hierarchy: Speculations on the Global Information Society" in *Information Technologies and Social Transformation*, (Bruce R. Guile, Ed.), National Academy Press: 1985, pp. 55 -79.

ContentGuard, "XrML:Extensible rights Markup Language", 2000.
http://www.xrml.org

Cox, Brad, Superdistribution: Objects as Property on the Electronic Frontier, *Addison-Wesley: 1996.*
http://www.virtualschool.edu/cox/IEEE97.html

Cox, I. J., J. Killian, T. Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Images, Audio and Video", *Proc. IEEE Internatinal Conference on Image Processing (ICIP '96)*, Sept. 1996, III., pp. 223-226.

Degenhart Drenth, B., "Building on the mda SPECTRUM-XML DTD for collections Management Data Interchange", *Museums and the Web 2001*, Archives and Museum Informatics: 2001.
http://www.archimuse.com/mw2001/papers/degenhart/degenhart.html

Digimarc Corp., "Frequently Asked Questions about Digimarc Signature Technology"
http://www.digimarc.com/imaging/faq.shtml

Digimarc Corp., "MarcSpider™", 2001.
http://www.digimarc.com/imaging/prspider.htm

"Digital Image Access Project, RLG Meeting, March 31-April 1, 1995", Archives and Museum Informatics, 9 (2), 1995. pp. 199-209.

EVA, (European Visual Archive Project), "Report on copyright issues", 1999.
http://www.eva-eu.org/WP41.PDF

(Fahn, Paul), "Answers to Frequently Asked Questions about Today's Cryptography", RSA Laboratories, 1993.

"Gallery V (for Virtual) Berea College Museum",
http://www.berea.edu/GalleryV/ExhibitsHome.html

Gross, R., "Librarian of Congress Unable to Preserve Fair Use in Digital Age", *EFFector* 13.11, (Dec.), 2000.
http://www.eff.org/effector/

Gurrian, E., "A Blurring of Boundaries", *Curator*, 38 (1), 1995. pp. 31-38.

Halfhill, T., and S. Salamone, "Components Everywhere, Microsoft's Network OLE and the OMG's CORBA are competing to distribute components on your network", *Byte*, Jan. 1996.
http://www.byte.com/art/9601/sec8/art8.htm

Hallacy, Marla, "The Dissemination of Art in the Technological Age", 2000
http://www.ukans.edu/~cybermom/CLJ/hallacy/hallacy.html

Harris, Lesley Ellen, *Canadian Copyright Law* , 3rd Ed., McGraw-Hill, 2000

Hartung, Frank, "WWW References on Multimedia Watermarking and Data Hiding Research & Technology", August, 1999.
http: //www-nt.e-technik.uni-erlangen.de/~hartung/watermarkinglinks.html

Hartung, F., and B. Girod, "Fast Public-Key Watermarking of Compressed Video", *Proceedings IEEE International Conference on Image Processing (ICIP 97)*, Santa Barbara, October 1997. pp. 528-531.

Hartung, F., J.K. Su, and B. Girod, "Spread Spectrum Watermarking: Malicious Attacks and Counter-Attacks", *Proceedings of SPIE Vol. 3657, Security and Watermarking of Multimedia Contents*, San Jose, CA, January 1999. pp. 147-158

Hoffert, P., T. Jurenka, B. Silverman, P. Spurgeon, and L. White, "Managing Intellectual Property in Digital Formats", *Forum for Inter-Industry Requirements for Technology-Based Intellectual Property Management*, U. S. Copyright Office and Interactive Multimedia Association, Washington, D. C., March 1996.

Hockin, Nora, "Canada's Digital Collections: Youth Employment Opportunities and Canadian Content On-Line", *Museums and the Web*: 2000
http://www.archimuse.com/mw2000/papers/hockin/hockin.html

IBM, "Watermarks: Protecting the image", 1996
http://www.research.ibm.com/image_apps/watermark.html

Internet Archive, "The Internet Archive: building an 'Internet Library'" (March 15, 2000)
http://www.archive.org/about/index.html

Johnson, R. C., "JPEG2000 wavelet compression spec approved", *EE Times*, Dec. 29, 1999.
http://www.eet.com/story/OEG19991228S0028

Jurenka, T., and P. Roosen-Runge, "Intercom Ontario: a residential multimedia distribution system in operation", presented at *Multimedia to the Home, Bandwidth Battles*, Saskatoon, August, 1997.

Kesse, Erich, "Negotiation and Documentation of Distribution Rights for Imaged Resources", University of Florida, 1994.
http://palimpsest.stanford.edu/bytopic/repro/kesse/negotiat.txt

King, Brad, " Fight Rages Over Digital Rights", *Wired Digital*: Jan. 16, 2001
http://www.wired.com/news/politics/0,1283,41183,00.html?tw=wn20010116

Koenen, R., "MPEG4-4, Multimedia for our time", *IEEE Spectrum*, 36, (2), 1999. pp. 26-33.

Kutter, M. and F.A.P. Petitcolas, "A fair benchmark for image watermarking systems."In *Proceedings of Electronic Imaging '99, Security and Watermarking of Multimedia Contents*, (P. W. and E. J. Delp, eds.), Society for Imaging Science and Technology and International Society for Optical Engineering , 1999. pp. 226—239.

Lehmann-Haupt, John, "Chained Melodies", Think Research Magazine, *(2), 2000.*
http://www.research.ibm.com/resources/magazine/2000/number_2/solutions200.html

(Lesk, M.), "Humanities and Arts on the Information Highways, Working Group Reports: The Technical Challenge for the Humanities and Arts", Coalition for Networked Information, Final Report 1994
http://www.cni.org/projects/humartiway/humartiway-rpt.part2.html#tc

"Licensing Still Images", Timestream Inc., 1994.

Macq, B., and J.-J. Quisquater, "Digital Images Multiresolution Encryption", IMA IP-Workshop, 1994.
http://www.cni.org/docs/ima.ip-workshop/Macq.Quisquater.html

Maître, H., "Image Waternarking, Why is watermarking a hard problem.", Korea-France Workshop on Multimedia, Seoul, Korea, (July 6-9), 1998.

Microsoft, "Window media Rights Manager 7", May, 2000.
http://www.microsoft.com/windows/windowmedia/enWM7/rightsmanager.asp

Mintzer,F., G. Braudaway, F. Girodano, J. Lee, and K. Magerlein, "Populating the Hermitage Museum's New Web Site", IBM Research Report, RC21753 (97990), IBM: 2000.

MIRADOR, "MPEG-4 Intellectual Property Rights by Adducing and Ordering", ACTS: 1999.
http://www.infowin.org/ACTS/RUS/PROJECTS/ac302.htm

National Palace Museum – Taiwan, Virtual Exhibits
http://www.npm.gov.tw/english/live/live.htm

Norman, S., "Copyright in the Global Information Infrastructure (GII), Mexico, 22-24 May 1995", *IFLA Journal* , 21 (3), 1995.

Orlowski, A., "The Open PC is dead - start praying, says HD guru", The Register, 7 March 2001.
http://www.theregister.co.uk/content/2/17419.html

Parks Canada, "Image Use"
http://parkscanada.pch.gc.ca/Schoolnet/PCimages/homepage/homepage_e.HTM

Petitcolas, F., "Weakness of existing watermarking schemes, StirMark" (1997)
http://www.cl.cam.ac.uk/~fapp2/watermarking/image_watermarking/stirmark/index.html

Petitcolas, F., "The information hiding homepage - digital watermarking & steganography", 2000.
http://www.cl.cam.ac.uk/~fapp2/steganography/

Petitcolas, F., "Watermarking and Steganography – Companies & Products", University of Cambridge, 1998.
http://www.cl.cam.ac.uk/~fapp2/watermarking/products.html

Petitcolas, F. and R. Anderson, "Evaluation of copyright marking systems". In *Proceedings of IEEE Multimedia Systems*, vol. 1, 1999. pp. 574—579.

Resnick, P. "Platform for Internet Content Selection", W3C, Jan. 1998.
http://www.w3.org/PICS/

(Reuters), "Gates' Corbis buys giant photo agency", June 15, 1999.
http://www.zdnet.com/zdnn/stories/0,4586,2276787,00.html

Rottenberg, B., and R. Pantalony, "Moral Rights and Exhibition Rights, A Canadian Museum's Perspective"; Copyright and Fair Use, The Great Image Debate, *Visual Resources*, Gorden and Breach, 1997. p. 409

Rowan, G., "Secure computer files may not be so safe", *Globe & Mail*, Dec. 4, 1997, p. B8

Santa Cruz, Diego, "Watermark tests in JPEG2000", Signal Processing Laboratory, Swiss federal Institute of Technology, 1999.
http://eurostill.epfl.ch/~ebrahimi/JPEG2000Seminar/SantaCruz.pdf

Schneier, B., *Secrets and Lies, Digital Security in a Networked World*, Wiley: 2000.

Schneier, B., "Hard-Drive-Embedded Copy Protection", *Crypto-Gram*, Feb. 15, 2001.
http://www.counterpane.com/crypto-gram-0102.html#1

Schofield, J., "The Fight for Knowledge", *Macleans*, Dec. 4, 2000.
http://www.macleans.html.ca/xta-asp/storynav.asp?/2000/12/04/Education/44105.shtml

Smith, B., and D. Semperger, "The Power of Digital Archiving with Photo CD", *Spectra* 22 (3), Winter 1994-95, p. 15.

Snow, M., "License to Kill? Copyright Ownership and Fair Use in Age of Licensing", VRA, July 1997.
http://www.oberlin.edu/~art/vra/license.html

Spurgeon, G. (<gspurgeo@SPIFF.CHIN.GC.CA>), "Re: artists' rights in Canada", posting to MUSEUM-L, 11 April, 1996.

State Hermitage Museum, St. Petersburg, Russia. 'Digital Hermitage Project'
http://www.hermitagemuseum.org/

Stefik, M., "Trusted Systems", *Scientific American*, March 1997.
http://www.sciam.com/0397issue/0397stefik.html

Stewart, Doug. "Masterieces on View", IBM Research Magazine, *number 2, 1999*
http://www.research.ibm.com/resources/magazine/1999/number_2/solutions299.html

Storm, W., "The value of integrated access to print and AV collections", *IFLA Journal* 21 (3), 1995. pp. 203-210.

Strong, William S., "Copyright in the New World of Electronic Publishing"
Electronic Publishing Issues II, Association of American University Presses, (AAUP) Annual Meeting, *Washington, D.C., June 17, 1994.*
http://www.press.umich.edu/jep/works/strong.copyright.html

Szczesny, Barry G., "What's Happening in Washington" , American Association of Museums Annual Meeting Presentation, April 1999.
http://www.panix.com/~squigle/rarin/corel2.html

Tomlin, Judith, "Digitization at the Canadian Museum of Civilization: A View From the Shop Floor" *International Committee for Documentation (CIDOC) of the international Council of Museums, Annual Meeting*, Ottawa, ON Aug 23 – 24 ,2000.
http://www.chin.gc.ca/Resources/Cidoc/English/Presentations/jtomlin.html

"RightsMarket™", Technical White Paper

Trant, J., "The Museum Educational Site Licensing Project", *Spectra*, 22, Winter 1994-95, pp. 19-21.
http://ei.cs.vt.edu/~mm/cache/Trant.htm

University of Alberta, AMICO Site License
http://ej.library.ualberta.ca/database/index.cfm?ID=71

"Van Eyck Project", Visual Arts Network for the Exchange of Cultural Knowledge (VASARI)
http://www.vasari.co.uk/van_eyck.htm

van Horik, René , "Archives and Photographs: the 'European Visual Archive' Project (EVA)", *Cultivate Interactive* (3) , 2001.
http://www.cultivate-int.org/issue3/eva/

Voyatzis, G., and I. Pitas, "Protecting Digital-Image Copyrights: A Framework", *IEEE Computer Graphics and Applications*, January/February 1999, pp. 18-24.

Walter, Mark, "Keeping tabs on the taking and selling of digital images", *Seybold Report on Publishing Systems*, 24, Jan 2, 1995, pp. 21+.

Weber, Hartmut, "Opto-Electronic Storage—An Alternative to Filming?" Commission on Preservation and Access, *Newsletter*, (Feb.), 1993.

WIPO (World Intellectual Property Organization) Copyright Treaty, Geneva, 1996.
http://www.wipo.org/eng/diplconf/distrib/94dc.htm

Zhao, J., "Applying Digital Watermarking Techniques to Online Multimedia Commerce", *Proc. of the International Conference on Imaging Science, Systems, and Applications (CISSA '97)*, 1997.
http://syscop.igd.fhg.de/Publications/Zhao97a.pdf

Vendors and Organizations

Alchemedia Technologies, Inc.
300 De Haro Street, Suite 334, San Francisco, CA 94103 USA
Tel: 1-800-561-8295
http://www.alchemedia.com/

BELLE Project
http://www.netera.ca/belle

Bridgeman Art Library,
17-19 Garway Road, London W2 4PH UK
Tel: +44 (0)20 7727 4065
email: info@bridgeman.co.uk
http://www.bridgeman.co.uk/

Cognicity,
7171 Ohms Lane, Suite 100
24947 Lorena Drive Minneapolis, MN 55439 USA
Tel: 952-841-7100
Fax: 952-841-7101
Email: info@cognicity.com
http://www.cognicity.com/

ContentGuard, Inc.,
6500 Rock Spring Drive, Suite 110 Bethesda, MD 20817-1105 USA
Tel: 1-800-870-0705
Tel: 1-650-813-7886 (Outside of the USA)
http://www.contentguard.com

Corbis Corporation,
15395 SE 30th Place, #300, Bellevue, WA 98007 USA.
Tel: (206) 641-4505
Fax: (206) 643-9740
http://www.corbis.com

Dryden Aircraft Research Aircraft Photo Archive,
Email: robert.binkley@dfrc.nasa.gov
http://www.dfrc.nasa.gov/gallery/photo/

Fraunhofer-Institut für Graphische Datenverarbeitung ,
Rundeturmstraße 6, D- 64283 Darmstadt Germany.
Tel: + +49 / 6151 / 155-0
Fax : + +49 / 6151 / 155-199
http://www.igd.fhg.de/
Dr. Eckard Koch
Tel.: (06151) 155-147.
Fax: (06151) 155-199.
Email: ekoch@igd.fhg.de

IBM DB2 Digital Library Project
http://www-4.ibm.com/software/is/dig-lib/casestudy.html

InterTrust Technologies Corporation
4750 Patrick Henry Drive Santa Clara, CA 95054 USA.
Tel: 1 (800) 393-2272 (within U.S.)
Tel: + 1 (408) 855-0100 (outside U.S.)
Fax: + 1 (408) 855-0144
Email: info@intertrust.com
http://www.intertrust.com

MediaSec Technologies LLC,
321 South Main Street, Suite 100, Providence, RI 02903 USA.

Tel: +1-401-831-2479
Fax: +1-401-453-0444
Email: info@mediasec.com
http://www.mediasec.com

OnDisC Research Group
Sheridan College, Office of Research Development, 407 Iroquois Shore Road, Rm. A-23 Oakville, Ontario Canada.
http:// www.ondisc.ca

RightsMarket,
500, 700 - 4th Avenue S. W., Calgary, Alberta T2P 3J4 Canada.
Main Reception: (403) 571-1835
Fax: (403) 571-1838
Sales: 1 (877) 543-3556
Email: sales@rightsmarket.com
http://www.rightsmarket.com/

Superdistribution™, Inc.,
11800 Sunrise Valley drive, Suite 1000, Reston, Virginia, 20191, USA.
Tel: 703-244-0986
Email: info@superdistributed.com
COO: Finley Foster
Email: ffoster@superdistributed.com
http://superdistributed.com

VASARI Enterprises
44A Florence Road, Fleet, Hampshire, GU13 9LQ UK.
Tel: + 44 [0] 20 8977 7858
Fax: + 44 [0] 20 8943 9256
Email: jamesrhemsley@cix.co.uk
http://www.vasari.co.uk

Vyou.com
2 North Second Street, Suite 1450, San Jose, California 95113 USA.
Tel: (408) 287-4200
Fax (408) 279-5643
Email: info@vyou.com
http://www.vyou